View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by ScholarWorks@UMass Amherst

University of Massachusetts Amherst

ScholarWorks@UMass Amherst

Doctoral Dissertations

Dissertations and Theses

Summer November 2014

Receiver Design and Security for Low Power Wireless Communications Systems

Kyle A. Morrison

Follow this and additional works at: https://scholarworks.umass.edu/dissertations_2

 Part of the Electrical and Computer Engineering Commons

Recommended Citation

Morrison, Kyle A., "Receiver Design and Security for Low Power Wireless Communications Systems" (2014). *Doctoral Dissertations*. 242.
https://doi.org/10.7275/n4vf-1w67 https://scholarworks.umass.edu/dissertations_2/242

This Open Access Dissertation is brought to you for free and open access by the Dissertations and Theses at ScholarWorks@UMass Amherst. It has been accepted for inclusion in Doctoral Dissertations by an authorized administrator of ScholarWorks@UMass Amherst. For more information, please contact scholarworks@library.umass.edu.

RECEIVER DESIGN AND SECURITY FOR LOW POWER WIRELESS COMMUNICATIONS SYSTEMS

A Dissertation Presented

by

KYLE ANDREW MORRISON

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

DOCTOR OF PHILOSOPHY

September 2014

Electrical and Computer Engineering

© Copyright by Kyle Andrew Morrison 2014

All Rights Reserved

RECEIVER DESIGN AND SECURITY FOR LOW POWER WIRELESS COMMUNICATIONS SYSTEMS

A Dissertation Presented

by

KYLE ANDREW MORRISON

Approved as to style and content by:

Dennis L. Goeckel, Chair

Patrick A. Kelly, Member

Marco F. Duarte, Member

Thurlow Cook, Member

Christopher V. Hollot, Department Chair
Electrical and Computer Engineering

ACKNOWLEDGMENTS

The completion of this dissertation marks the end of a delightful, enlightening and rewarding journey where I transition into a new stage: employment with MIT Lincoln Laboratory. I greatly thank everyone I've come into contact with over my graduate studies because you have helped shape my graduate experience.

I would like to first and foremost express my deep appreciation and gratitude to my advisor Professor Dennis Goeckel, for his patient guidance and mentorship throughout my time as a PhD student. I often recall entering research meetings uncertain but then leaving empowered and confident. It has been his passion, motivation, work ethic and shared experiences that have been a huge inspiration in my life and it was truly an honor and privilege to have worked with him. His intellectual heft is matched by only his genuinely good nature and willingness to assist, and, for all of this and more, I am deeply indebted.

Thank you to my dissertation committee, Professors Patrick Kelly, Marco Duarte and Thurlow Cook, for the insightful questions, comment and feedback to my dissertation. I would like to thank the Northeast Alliance for Graduate Education and the Professoriate (NEAGEP) for funding, mentorship, and monthly dinners that brought a sense of community with other fellows, as well as lifetime friendships. Professor Sandy Peterson has been influential during my time in graduate school, has always made herself accessible, given more time and energy than I thought was possible for a person to give, and has been a friend, which could be foreshadowed by the four-hour conversation we had on my first visit to Umass.

Dr. Kenneth Durgans and Dr. Michael Silas, thanks for being advocates dedicated to fostering leadership and the motivation to pursue a graduate degree. I

thank my fraternity brothers of Kappa Alpha Psi for serving as a foundation and assisting me to live up to the motto of "Achievement in Every Field of Human Endeavour". Thanks to the friends that I have made over the years in the Amherst community for the extraordinary experiences. Also, thanks to my longtime Rensselaer Polytechnic Institute (RPI) friends for the memorable times, fulfilling the RPI slogan, "Why not change the world?" I greatly appreciate my labmates for creating a fun and conducive work environment; monthly gatherings outside of the lab helped to strengthen bonds.

Finally, the one person who has spent more time with me than anyone else while in graduate school, my fiancé Idalys Rivera has provided unwavering support through the peaks and the valleys. You continually brightened my life and have been a catalyst for the motivation to succeed. I thank my parents for the sacrifices they have made for the investments into my future, and constant exposure to opportunities that they did not have. My parents have always been one of my biggest supporters and continually show unconditional love. My sisters and brothers are, simply put, quite amazing; the relationships that we have shared have helped shape me.

This dissertation is based in part upon work supported by the National Science Foundation under Grant ECS-0725616, NeTS-1018464, CNS-0831133 and by the STTR Program of the Army Research Office.

ABSTRACT

RECEIVER DESIGN AND SECURITY FOR LOW POWER WIRELESS COMMUNICATIONS SYSTEMS

SEPTEMBER 2014

KYLE ANDREW MORRISON

B.Sc., RENSSELAER POLYTECHNIC INSTITUTE

Ph.D., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Dennis L. Goeckel

This dissertation focuses on two important areas in wireless communications: receiver design and security. In the first part of this dissertation we consider low data rate receiver design for ultra-wideband (UWB), a wideband radio technology that promises to help solve the frequency allocation problem that often inhibits narrowband systems. Reference-based receivers are promising candidates in the UWB regime, because the conventional rake receiver designs suffers from complexity limitations and inaccuracies in channel estimation. Many reference-based systems have arisen as viable solutions for receivers. We unify these systems as well as other systems into the general framework for performance analysis to suggest the optimal system for varying constraints. We improve the performance of frequency-shifted reference (FSR-UWB) for an average power constraint by halving the frequency offset and employing a sample-and-hold approach across the frame period. Also, we introduce a novel peak mitigation technique; tone reser-

vation, for the multi-differential (MD) version of FSR-UWB, to reduce the high peak-to-average power ratio observed as the data carriers increase.

The next part of this dissertation is about wireless security which is ubiquitous in modern news. Cryptography is widely use for security but it assumes limited computational abilities of an eavesdropper, is based on the unproven hardness of the underlying primitives, and allows for the message to be recorded and decrypted later. In this dissertation we consider an information-theoretic security approach to guaranteeing everlasting secrecy. We contribute a new secrecy rate pair outage formulation, where an outage event is based on the instantaneous rates of the destination and the eavesdropper being below and above desired thresholds, respectively. In our new secrecy rate pair outage formulation, two new unaccounted outage events emerge: secrecy breach, where the eavesdropper is above the targeted threshold; unreliable, where the destination is unable to successfully decode the message. The former case must be carefully avoided, while for the latter case we can exploit automatic retransmissions (ARQ) while maintaining the eavesdropper intercept probability below the target threshold. We look at both "simple" receivers and also complex receivers that use a buffer to store previous messages to maximally combine signal-to-noise ratio (SNR). Then we extend these results to the two-hop case where we maximize the end-to-end secure throughput by optimizing the intercept probability at each eavesdropper given a total end-to-end intercept constraint. Lastly, we consider the difficult case in information-theoretic security: the near eavesdropper case, where we contribute an optimal power allocation algorithm that leverages nearby chatter nodes to generate noise to reduce the probability of intercept by the eavesdropper while minimally impeding the source-to-destination communication. As shown in both one-hop and two-hop cases, allowing a slight outage at the destination for cases of when the eavesdropper is above a specific threshold greatly improves secrecy performance.

TABLE OF CONTENTS

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

CHAPTER 1

INTRODUCTION

1.1 Motivation

Wireless communication is widely employed because of its flexibility and ease of use, in particular allowing mobility of the users. Advancements in wireless communications have focused on reliability, robustness, speed, minimizing cost and power. Recently, ultra-wideband (UWB) was seen as an emerging area in wireless communication; in this dissertation, we provide a comprehensive framework for low-to-moderate data rate reference-based UWB systems. We consider the comparison of reference-based UWB systems under various constraints, optimizing frequency shifted reference (FSR-UWB) for an average power constraint and then the multi-data version of FSR-UWB (multi-differential (MD-FSR)) for a peak power constraint.

More recently, an area in wireless communications that has attracted significant interest is security, in particular physical-layer security. Security is a vital concern because information intercepted can have a damaging effect on users, such as identity theft, ruined reputation, revenue lost and stolen intelligence. Hence it is very important to formulate a secure system that guarantees everlasting protection from an eavesdropper. This dissertation considers new secrecy outage formulations involving jamming and automatic request retransmission (ARQ) techniques that help improve reliability and security in wireless communication systems. We will consider the case of when the eavesdropper uses a complex receiver, where it buffers previous transmissions and soft combines for an additional advantage

at intercepting the message. Also we consider the difficult problem of the "near eavesdropper" case, optimally allocating power to chattering nodes and optimizing the outage constraint at the destination to further reduce the end-to-end intercept probability constraint.

1.1.1 Ultra-wideband

Frequency allocation for the wide bandwidths required for very high data rates or accurate positioning systems has been a growing concern in wireless communication. The scarcity in available contiguous frequency for such is one of the main motivations for ultra-wideband (UWB). UWB has the ability to co-exist with other technologies because its signal energy is spread over a larger bandwidth than narrowband systems, and its interference to other more narrowband systems that occupy the same frequency band is minimal due to its low spectral density. Thus, in 2002 the Federal Communications Commission (FCC) designated the $3.1 - 10.6$ Ghz spectrum for UWB radio applications, where the bandwidth of the system is at least 20% of the center frequency or larger than 500 Mhz. Because of the extremely large bandwidth of UWB, an added advantage is diversity against multipath, and the ability to carry very high date rates. Hence, UWB communication systems have been considered for standardization for short range low-power wireless communications in both high data rate (IEEE 802.15.3 [1]) and low-to-moderate data rate (IEEE 802.15.4a [2]) applications.

However the large bandwidth increases the receiver complexity because of the large number of resolvable paths as well as the precision required for channel estimation. Hence, standard coherent rake receivers [3] become infeasible. This motivated researchers to look into other receiver alternatives, mainly noncoherent systems. The initial noncoherent system proposed was Transmitted-Reference (TR) [4]. TR-UWB was an attractive alternative to the traditional rake receiver design

but was not readily accepted because of the inability to build a wideband delay line in integrated circuits. To address this problem, Frequency Shifted Reference (FSR)-UWB [5] was introduced, where translation is done in the frequency domain rather than the time domain, in which case the delay line can be replaced by a mixer. During the FSR-UWB prototype construction [6], the undergraduate team that built the FSR-UWB prototype recognized that the sinusoid that separated the reference and data waveforms could be replaced with a square wave, which results in pulse position modulation (PPM)-UWB. This observation led to the first framework of simple reference-based systems [7]. Independently researchers proposed Code Shifted Reference (CSR)-UWB [8] and Code-Multiplexed (CM)-UWB [9], which use orthogonal codes to represent the data and reference signals.

In this dissertation we first contribute an extension to the framework of [7]. Reference-based systems, including multi-data and multi-user systems, are put into a unified framework, and performance analysis is done to obtain the potential optimal set of waveforms as well as to help aid in comparison of the well-known systems. This framework indicates the choice of constraint has a significant impact on the choice of the number frames per bit, which is a critical parameter when considering reference-based systems. We optimize under two constraints:

1. *Average power:* We optimize reference-based systems under an average power constraint, restricting to a small number of frames per bit. This optimization leads to burst mode PPM as the optimal performing waveform given an average power constraint, indicating FSR-UWB has worse performance than PPM-UWB and CSR/CM-UWB. Therefore two solutions were sought to improve FSR-UWB system performance :

   (a) A sample-and-hold technique was used across each frame to minimize signal degradation, as discussed in detail in Chapter 2.

(b) We noted that the frequency offset between the data and reference signal can be halved, thus reducing the slight degradation that occurs as the data rate approaches the coherence frequency of the channel.

These above solutions led to enhanced system performance for FSR-UWB, very comparable to PPM-UWB.

2. *Peak power:* Peak power is of great concern in low-power integrated circuitry for a UWB transmitter [10]. Similar to the average power case, we optimized under the general framework for reference-based systems and determined the optimal waveforms under a peak power constraint. For a large number of frames FSR-UWB showed promising performance especially as the data rate increases (multi-differential (MD)-FSR), but, as the number of frames increase, it can introduce high inter-frame interference (IFI). We established a peak mitigation technique for MD-FSR under the following constraints:

   (a) Does not reduce the data rate.

   (b) Does not increase complexity and affect system performance.

   The solution under these constraints yields a tone reservation tactic similar to that from orthogonal frequency division multiplexing (OFDM), where additional peak reduction carriers are used to alleviate the peak-to-average power ratio (PAPR) of the transmitted signal. Because of the unusual constraints on the data rate of the MD-FSR-UWB system, there is no loss in data rate due to tone reservation as in a standard OFDM system.

1.1.2 Physical Layer Secrecy

The wireless communication medium makes it very susceptible to eavesdroppers (unintended receivers). Traditional methods to alleviate the issues of an eaves-

dropper are done using some form of cryptography, with a private key exchange between the intended users that is unknown to all unintended users.

A strong advantage of physical layer security is that it does not rely on limited computational abilities of the eavesdropper; rather, it relies on the physical channel quality, as the secrecy capacity is given by the difference in the capacities between the main channel and the eavesdropper channel. However, on wireless communication channels, the randomness of the fading gains makes it impossible to guarantee secrecy over every instantiation of the fading, hence motivating the concept of secrecy outage. The instantaneous capacity is defined as the maximum rate of information that can be reliably transmitted between Alice and Bob conditioned on the fading, noted as R_B; likewise, between Alice and Eve, R_E. The secrecy outage is generally defined as the probability the instantaneous secrecy capacity ($R_S = R_B - R_E$), the difference between the instantaneous capacity of the Alice and Bob (R_B) channel and that of the Alice and Eve (R_E) channel, is less than the targeted secrecy rate (R_0) [11, 12].

Hence for a secure system, the standard definition states that secrecy is achieved when the secrecy rate (R_S) is above the designed secrecy rate ($R_S \geq R_0$). However, this construction is flawed: the wiretap construction [13] requires a rate *pair* (R_B, R_E), and there does not exist a universal rate pair that guarantees secrecy over the whole targeted secure region. This motivates the definition of two hazardous regions that are unaccounted for in the standard formulation: the region where R_{E0}, the target eavesdropper rate is above R_E, where secrecy is compromised; and R_{B0}, where the target destination rate is below R_B and the system is unreliable. In this dissertation we offer a tighter definition of secrecy outage and form a different secrecy outage formulation, where we consider not only choosing a target secrecy rate that represents the difference between the main channel and eavesdropper channel, but rather the choice of two individual target secrecy rates.

1. Rather than one degree of freedom, R_0, as in the outage formulation shown in, for example, [11], we introduce two degrees of freedom (R_{B0}, R_{E0}) for a system not to be an outage; in other words, Bob must be able to decode the message while Eve is unable to decode the message. The secrecy outage definition of [11] is sufficient if R_B or R_E is known, in which case the choice of R_0 fixes the other rate (R_{E0} or R_{B0}, respectively) and hence specifies the pair, in which case our definition is equivalent to the prior definition. However, if neither R_B nor R_E is known (i.e no channel state information at the transmitter [11, pg 199]), then we would argue that a stricter definition is required. Interception of the message ($R_E > R_{E0}$) is more important than simply the dropping of the packet ($R_B < R_{B0}$, in which retransmission can be employed). In particular, we can exploit the use of automatic repeat request (ARQ) schemes [14], keeping the eavesdropper intercept probability below the outage constraint while maximizing throughput to the destination. This dissertation explores two widely used hybrid ARQ systems: basic hybrid ARQ, where there is no memory and the receiver only provides the source with a single bit of feedback telling whether the packet was receive correctly, and hybrid ARQ with soft combining, where the receiver also buffers receptions and uses packet combining over multiple transmissions to increase the SNR of the received message.

2. In addition, we consider the case where there are other nodes (relay or noise generators) in the network outside of the source, destination and eavesdropper. We introduce a protocol where system nodes that are not employed as relay nodes and that have a bad channel to the receiver (and hence will not interfere significantly with the message transmission), transmit random noise (chatter) to confuse the eavesdropper. Given channel state information between all pairs of system nodes, it is possible to keep the destination

out of outage if the aggregate chatterer power impinging on the receiver is constrained. This forms a constraint on the chatterer power, and we then investigate the optimal allocation of this power budget to the noise generating nodes, which we call "chattering nodes", with the goal of maximally degrading the eavesdropper signal. More formally, we guarantee a desired signal-to-interference plus noise ratio (SINR) at the destination while maximizing the probability that the eavesdropper cannot meet its (often lower) SINR threshold. The problem formulation leads to a *water-filling* result, where we allot power to chatterer nodes that are close to the eavesdropper and far from the destination, or whose signal will be badly faded when it arrives at the destination.

1.2 Background

1.2.1 Ultra-wideband

The first wireless systems were at line of sight distances via smoke signals, torch signaling, flash mirrors, signal flares or semaphore flags (rudimentary signals). In 1838 Samuel Morse contributed the Telegraph Network, and eventually the telephone network replaced the telegraph network. In 1895, Marconi demonstrated the first radio transmission from Isle of Wight to Tugboat, a distance of approximately 18 miles, thus giving birth to radio communications. The most important factors in radio technology are: transmission of information over large distances, better quality, minimum power, small and cheap devices.

One of the most successful application of wireless networking is the cellular telephone system. In 1915 the first voice transmission between New York and San Francisco was demonstrated. Gradually in 1946, the cellular system was made public across 25 cities in the U.S. Unfortunately due to inefficient use of the radio spectrum, the system capacity was limited. For example, 30 years into the matura-

tion of the technology, there was only support for approximately 543 users. Then, later in the $50's$ and $60's$ AT&T Bell labs exploited the fact that the power of the transmitted signal falls off with distance, allowing multiple users to communicate at the same frequency at spatially separate locations with minimal interference, and thus greatly improving efficient spectrum use. In modern communications, technology such as code division multiple access (CDMA) has helped greatly to advance cellular technology. Frequency allocation is a major concern in narrow band systems because of the limited availability of bandwidth. In 2002 UWB, a wideband technology was proposed as a solution to resolve the frequency allocation problem. UWB was defined as unallocated frequency spectrum in $3.1 - 10.6$ GHz in the U.S.A. with a power limit of $41.3 dBm/MHz$, operating in the noise floor and coexisting with narrowband systems. UWB offers many advantages such as higher data rate, multi users, fine time resolution, and high performance in a multipath environment. However building a wideband receiver is no trivial task.

The natural approach to UWB receiver design is to apply a rake receiver similar to that seen in traditional wideband wireless systems. But, because UWB systems spread energy over a large bandwidth, a rake receiver implementation is difficult because of the channel estimation required to support a large number of taps [3]. In addition, these taps come at the high price in circuit area and complexity [15]. This motivated further research for an alternative receiver design with low complexity [16].

An early solution offered was the transmitted reference (TR-UWB) system [4, 17]. In a UWB system, a symbol period is generally divided into some number of frames, each containing a single UWB pulse. In the original TR-UWB system, two pulses are transmitted per frame: a reference pulse and a data pulse. These pulses are separated by a known delay, generally selected to be larger than the delay spread of the channel. The relative polarity of the reference and data pulses

indicates the information bit: the bit is 0 if they have the same polarity and 1 if there polarity differs. Since the reference and data go through approximately the same channel, the reference serves as a noisy template for the channel distorted data signal. Correlation is conceptually simple at the receiver, hence allowing for efficient collection of the received signal energy. However, a wideband delay element is required, which is difficult to implement in low power integrated circuits [18].

An alternative receiver to the traditional rake receiver design and transmitted reference is frequency shifted reference (FSR)-UWB [7], where, instead of offsetting the data and reference signals in the time domain, translation is done in the frequency domain. An advantage of FSR is that a delay element is not required at the receiver, but instead a mixer is used.

Independently, research teams motivated by the FSR-UWB scheme proposed more general square-wave approaches: code-shifted reference (CSR)-UWB by Nie and Chen [8], and code-multiplexed reference (CM)-UWB by DAmico and Mengali [9]. In these schemes, rather than separating the reference and data with a frequency shift, the reference and data signals are modulated with unique code sequences from the rows of a Hadamard matrix and thus are offset by an orthogonal code shift. There are many possible code combinations between reference and data signal that maintain orthogonality but, for the single user case, choosing the optimal set of codes yields a system similar to the standardized 802.15.4a [2] version of pulse position modulation (PPM-UWB) [2].

In [19], multiple carriers, each carrying data differentially encoded relative to a single reference (called multi-differential (MD)), are employed. Orthogonality is preserved since the frequency offsets are well below the channel coherence bandwidth. This allows a strong reference with cost amortized over a number of data bits, which improves the performance of each of the data streams. In particular, if

K data signals are transmitted over K orthogonal carrier frequencies, MD-FSR has a $5\log_{10} K$ dB gain in performance in terms of average signal-to-noise ratio (SNR) over standard single-differential (SD) FSR; in the limit of large K, the reference becomes essentially noiseless, thereby eliminating the dominating noise cross noise term of reference-based systems and leading to a system whose performance is only a fixed energy loss worse than the coherent system whose implementation has proven so difficult [19].

The systems discussed above represent a small class of the possible waveforms for separating the reference from the data which can be used for a reference-based system. In a unified framework, performance analysis is done to obtain the potential optimal set of waveforms as well as to help aid in comparison of the well known systems. However, while considering this comparison, one thing that has become apparent is that the constraints under which systems are compared must be carefully considered. Hints of this dependence can be seen in the differing comparisons of [7], where FSR-UWB has shown to have optimality properties, for a large number of frames and [9], where CM-UWB was shown to significantly outperform FSR-UWB for a small number of frames.

1.2.2 Physical Layer Secrecy

Wireless communications is often preferred over wired communications because of scalability of installation, flexibility of setup, multi-user support and mobility. Contrary to wired communications where the signal is constrained to a wire or cable, in wireless communications the signal is broadcast over the air. Hence, the advantages wireless communications provides in flexibility and ease of use are also what makes it vulnerable because of the ease of unintended access to the signal by nearby nodes. Moreover systems such as the internet connect more than a billion devices in a network built with security as an afterthought.

The vulnerabilities and security holes, for example, of the internet stem from the fact of its fast growth. The system was first built for academic researchers and created an intimate environment for trusted individuals to share and access information and applications quickly. However the internet has grown to billions of users, and has evolved from its original intent, became a billion dollar business with commercial players, allowing for such services such as Electronic commerce (E-commerce), electronic mail (email) and the World Wide Web (WWW). In [20] it was shown that 47% of U.S. adults had their personal information exposed by hackers (eavesdroppers). For example, 70 million of Target customers' personal information, credit card and debit card information was stolen, and similar events happened with 33 million Adobe user credentials, 4.6 million Snapchat users' account data, and AOL's 120 million account holders. Another prominent attack "Heartbleed", which exploited a software bug in the OpenSSL cryptographic software library and forced computers to divulge secret information stored, has affected millions of people. Thus there needs to be systems and protocols in place so that we can make communications secure.

Security started out as an afterthought in the construction of the Open Systems Interconnection (OSI) (7-layer) model. However, in Internet applications security became a necessity because of the rise of malicious users. The network layer was identified as the place to handle security via cryptography. A commonly used example of cryptography is the source and destination establishing a key over an insecure channel, for example, via a Diffie-Hellman key exchange protocol [21]. The eavesdropper is at a significant computational disadvantage to decode the message because he/she does not know the secret integers chosen by the source and destination. Thus, cryptography assumes an eavesdropper can perfectly listen to the message but its computational abilities restrict it from correctly decoding the message; hence, eavesdroppers near the source are thwarted, which is of great

value in the wireless environment. However if an eavesdropper has infinite computational abilities or stores the message for later decryption, security might be compromised.

Shannon [22] presented secrecy from an information-theoretic and physical layer background where he first considered transmission over a noiseless channel. Shannon's work assumes the adversary has perfect reception of the message and infinite computational abilities. In this case, he concluded (quite negatively) that secrecy required a key as long as the message. In a continuation of Shannon's work, Wyner considered secrecy over a noisy channel and introduced the wiretap channel [13].

In the wiretap code construction, the secrecy capacity is of great importance, as it provides a measure of the amount of information that can be communicated securely: the difference in the capacities between the main channel (R_B) and the eavesdropper channel (R_E) [11], [23, 24]. Since the channel is wireless, the stochastic nature of the fading channel makes it impossible to guarantee secrecy over every instantiation of the fading motivating the concept of outage probability, the probability the instantaneous secrecy capacity ($R_S = R_B - R_E$), the difference between the instantaneous capacity of the Alice and Bob (R_B) channel and that of the Alice and Eve (R_E) channel, is less than the targeted secrecy rate (R_0) [11, 12]. Hence for a secure system, secrecy is achieved when the secrecy rate (R_S) is above the designed secrecy rate ($R_S \geq R_0$).

The wiretap code construction can achieve positive secrecy if the channel from Alice to Bob is better than Alice to Eve. But, if the channel from the source to the eavesdropper is better than the Alice to Bob, then secrecy may not be achievable, which can occur in wireless systems if the eavesdropper is close to the source (the "near eavesdropper" problem). One solution offered to the near eavesdropper problem was noise forwarding [25], where relay nodes send dummy codewords

independent of the source message to confuse the eavesdropper. Another solution offered was cooperative jamming [26], where nodes not used in the relay transmission of the message but in close proximity to the eavesdropper introduce artificial random noise to degrade the message received at the eavesdropper. Contrary to noise forwarding, cooperative jamming allows the relay to harm the eavesdropper more than it harms the receiver. In [26], it was shown that a non-zero rate of secrecy can be achieved regardless of the eavesdropper location. In [27], cooperative jamming techniques that introduce artificial noise are again used to achieve secrecy.

1.3 Contributions

1.3.1 Ultra-wideband

1. *Generalized framework for noncoherent UWB systems is introduced:* A unified performance analysis is performed to show how systems perform under a peak constraint system (large number of frames), and an average power constraint (small number of frames) and suggests optimality properties to guide system design.

    - *Improving FSR-UWB:* FSR-UWB suffers in performance when a small number of frames is considered (average power constraint). There are two solutions to improve system performance:

        (a) FSR suffers degradation in comparison to other reference-based systems because of a cosine term in the bit error rate performance. A solution used here was to sample the envelope at the beginning of each frame and hold that sample across the frame period, hence making it constant over the frame period. This modified FSR scheme improves performance at low-to-moderate SNRs, but can demon-

strate significant error floors due to waveform distortion at higher SNRs.

(b) As investigated in detail in [5], the frequency offset causes a performance degradation as the data rate approaches the coherence frequency of the channel. In [28], it is noted that the frequency offset of FSR-UWB can be halved to address this latter concern. The halved frequency offset scheme reduces the degradation of FSR-UWB and system performance is close to those seen in CSR/CM-UWB.

- *System Performance:* For a peak power constraint (large N_f), our analysis and [7] suggest a broad autocorrelation function $R_{\phi_k}(\tau)$ of the separating waveform would correspond with improved system performance. In the case of binary CM-UWB, as considered in [9], the optimal separating waveform corresponds to the burst-mode PPM, and is arrived at through a different derivation in [9]. Systems underneath a peak power constraint which corresponds to a large N_f have similar performance, and thus for the binary case, conclude that ease of implementation is the key differentiator. This points to CM/CSR-UWB approaches, which avoid not only the delay lines of TR-UWB but also the amplitude modulation of FSR-UWB.

- *Peak mitigation for multi data rate systems:* Peak power is of great concern for multi-data rate UWB systems, especially as the number of carriers get large, similar to that seen in OFDM systems. A commonly used technique in OFDM to alleviate this problem is tone reservation, where some of the carriers (tones) are reserved for peak reduction rather than carrying data, and the signal peak can be reduced by the selection of appropriate values on the reserved tones. It is important to note that the carriers do not affect the signal detection performance because they are

orthogonal to each other, but in OFDM the cost of applying tone reservation is a reduced data rate because the peak reduction carrying signals are interleaved with data carrying signals. We introduced peak mitigation alternatives that do not restrict the data rate and are effective for reference-based systems, most notably for the multiple data carrier version of frequency-shifted reference based system. The MD-FSR system was improved using tone reservation where peaky data signals were alleviated by peak reducing signals above the coherence frequency of the channel, thus causing no reduction of the data rate. Such peak mitigation techniques lead to small PAPR gains of frequency-shifted reference UWB versus code-multiplexed and code-shifted reference UWB systems.

1.3.2 Physical Layer Security

1. *Secrecy Rate Pair Outage Formulation:* A new outage formulation was contributed where we consider wiretap rate pair design under the secrecy rate pair outage constraint, maintaining separate rate thresholds for the channels to each of the destination (Bob) and eavesdropper (Eve).

    - *ARQ Design:* We designed an ARQ scheme to maximize throughput to Bob while constraining the intercept probability at Eve, while accounting for her ability to intercept the packet on the first or any retransmission (or, in the case of soft combining, some combination of the initial transmission and retransmissions).

    - *Relay Node with ARQ:* Thus far most work has consider the single hop case. A two-hop network is also of great importance, where a source node passes the message to a relay node, and the relay node passes the message to the destination. Differently from the single-hop network,

the relay node adds signal diversity, which is very important in physical layer wireless security. We extend our one-hop secrecy rate pair construction to the two-hop case: we place a secrecy constraint on the end-to-end intercept probability by Eve, while maximizing the end-to-end throughput. Also, we consider the optimal distribution of the end-to-end secrecy constraint to each link to maximize the secure throughput.

2. *Optimal Power Allocation of Jammers:* In the case of Eve, with a high intercept probability, jamming techniques via noise generating nodes are used to inhibit Eve's reception. Optimal power allocation to the systems nodes that generate random chatter can be achieved via a *water- filling* approach. In this scenario we consider the optimal allocation of this power budget to the noise generating nodes, with the goal of maximally degrading the eavesdropper signal. More formally, we guarantee a desired signal-to-interference plus noise ratio (SINR) at the destination while maximizing the probability that the eavesdropper cannot meet its (often lower) SINR threshold.

CHAPTER 2

REFERENCE-BASED ULTRA-WIDEBAND (UWB) RADIO

Ultra-wideband (UWB) radio is promising for localization and wireless communication, but receiver implementation difficulties due to the enormous bandwidth have slowed development of the technology. The first proposed reference-based system was the transmitted reference (TR)-UWB architecture, but TR-UWB is plagued by the difficulty in building an extremely wideband delay line in small integrated circuits. This difficulty lead to frequency shifted reference (FSR)-UWB, where signal translation at the receiver is done in the frequency domain with a mixer rather than the time domain via a wideband delay element. The FSR-UWB system further motivated code-shifted (CS) and code-multiplexed (CM) systems, where separation is done in the code domain with orthogonal binary codes, thereby removing the amplitude modulation required in the FSR-UWB system. In this Chapter we incorporate all of these architectures into one general framework, and introduce a peak mitigation technique similar to the tone reservation scheme employed in orthogonal frequency division multiplexing (OFDM) systems but without the cost in data rate. A comparison of reference-based systems under either peak or average power constraints is presented.

2.1 Introduction

First introduced in 2002, coexisting with narrowband systems that include GPS, IEEE 802.11 (WLAN), the FCC allocated $3.1 - 10.1$ GHz to ultra-wideband (UWB) communications to help solve frequency allocation problems that inhibit wireless

communications. UWB transmission is defined as a signal bandwidth that exceeds the lesser of 500 MHz or 20% of the center frequency. The transmit signal of UWB systems are low-power ultra-short information-bearing pulses, where signals must operate at the noise floor of other narrowband systems that occupy the band; thus, the power level must be below -41.3 dBm.

UWB systems provide a viable solution for common problems facing short-range, low-power wireless communications systems. In particular, UWB offers many potential advantages over conventional technology, since its extremely large bandwidth promises transmission at higher date rates, low cost and duty cycle, frequency diversity for combating multipath, and a high multi-user capacity. UWB is a compelling approach for localization because of its fine time resolution which can lead to accurate asset tracking and precession navigation. Another application of interest is in networking for short-range, high-speed access to the internet, where UWB can be a physical layer candidate for Wireless Personal Area Network (WPAN). And UWB can be employed in sensor networks where energy is often limited. These are just a few of the endless opportunities of UWB. Hence, UWB communication systems have been considered for standardization for short range low-power wireless communications in both high data rate (IEEE 802.15.3) and low-to-moderate data rate (IEEE 802.15.4a) applications.

UWB offers a number of system design advantages that include: free of sine wave carriers, does not require Intermediate Frequency (IF) processing, and operates at baseband. However, a big challenge is transmitter design. The pulse of choice is the Gaussian pulse mainly because it has the smallest possible time-bandwidth product of 0.5, which maximizes the range-rate solution, and is readily available from the antenna pattern.

The natural approach to UWB receiver design is to apply a rake receiver similar to that seen in traditional wideband wireless systems. In a rake receiver design,

signal energy can be collected from various multipath branches, where each calculate path delays and amplitude distortions so that you can combine SNR from each path to coherently make a decision on the received signals. But, because UWB systems spread energy over a large bandwidth, a rake receiver implementation is difficult because of the channel estimation required to support a large number of taps [3, 29]. In addition, these taps come at the high price in circuit area and complexity [15] for small power limited devices. This motivated further research for an alternative receiver design with low complexity [16].

An early solution offered was the transmitted reference (TR-UWB) system [4, 17, 30, 31, 32]. In a low-power UWB system, a symbol period is generally divided into some number of frames, each containing a single UWB pulse. In the original TR-UWB system, two pulses are transmitted per frame: a reference pulse and a data pulse. These pulses are separated by a known delay, generally selected to be larger than the delay spread of the channel. The relative polarity of the reference and data pulses indicates the information bit: the bit is 0 if they have the same polarity and 1 if their polarity differs. Since the reference and data go through approximately the same channel, the reference serves as a noisy template for the channel distorted data signal. Correlation is conceptually simple at the receiver, the received signal is multiplied by a delayed version of itself over the symbol interval, hence allowing for efficient collection of the received signal energy. However, a wideband delay element is required, which is difficult to implement in low power integrated circuits [18].

An alternative receiver to the traditional rake receiver design and transmitted reference is frequency shifted reference (FSR-UWB) [5], where, instead of offsetting the data and reference signals in the time domain, translation is done in the frequency domain. An advantage of FSR is that a delay element is not required at the receiver, but instead a mixer is used. An undergraduate team implemented

a FSR-UWB prototype [6], where they recognized that the sinusoid separating the reference and data signals could be replaced by a square wave. The result is a system that has energy in either the first half of the symbol interval or second half of the symbol interval, called "burst-mode" pulse-position modulation (PPM), hence being similar to the proposed 802.15.4a standard [2]. This observation led to the general framework for simple reference based systems in [7]. Independently, research teams motivated by the FSR-UWB scheme proposed more general square-wave approaches: code-shifted reference UWB (CSR-UWB) by Nie and Chen [8], and code-multiplexed reference UWB (CM-UWB) by D'Amico and Mengali [9]. In these schemes, rather than separating the reference and data with a frequency shift, the reference and data signals are modulated with unique code sequences from the rows of a Hadamard matrix and thus are offset by an orthogonal code shift. There are many possible code combinations between reference and data signal that maintain orthogonality but, for the single-user case, choosing the optimal set of codes yields again a system similar to the standardized 802.15.4a version of pulse position modulation (PPM-UWB) [9].

Some of the most promising extensions to FSR-UWB for improving performance versus an average power constraint suffer under a peak power constraint, most notably [33] and [34]. In [34], multiple carriers, each carrying data differentially encoded relative to a single reference (called multi-differential (MD)), are employed. Orthogonality is preserved since the frequency offsets are well below the channel coherence bandwidth. This allows a strong reference with cost amortized over a number of data bits, which improves the performance of each of the data streams. In particular, if K data signals are transmitted over K orthogonal carrier frequencies, MD-FSR has a $5 \log_{10} K$ dB gain in performance in terms of average signal-to-noise ratio (SNR) over standard single-differential (SD) FSR; in the limit of large K, the reference becomes essentially noiseless, thereby eliminating

the dominating "noise cross noise" term of reference-based systems and leading to a system whose performance is only a fixed energy loss worse than the coherent system whose implementation has proven so difficult [34]. Per above, the major limitation of MD-FSR is a high peak-to-average power ratio (PAPR). The multiple sinusoids with random data modulation essentially lead to a similar PAPR problem to that of orthogonal frequency division multiplexing (OFDM) systems.

The systems discussed above represent a small class of the possible waveforms for separating the reference from the data which can be used for a reference-based system. In a unified framework, performance analysis is done to obtain the potential optimal set of waveforms as well as to help aid in comparison of the well known systems. However, while considering this comparison, one thing that has become apparent is that the constraints under which systems are compared must be carefully considered. In particular, due to its noncoherent nature, reference based systems can provide the somewhat unusual (and somewhat unpleasing) feature of showing improved performance as data rate increases if performance is plotted versus the average signal-to-noise (SNR) ratio [35, 36]. As described in detail in [5], this is because the constraints for such a system must be carefully considered. The peak power drawn from the transmitter pulse generator is often limited and corresponds to the cost in terms of battery life. Hence, we will take peak pulse power as an important energy constraint. However, this is not the only constraint, because the FCC provides a spectral mask below which the power of the signal must lie. Once the transmitter pulse shape is set, compliance with this spectral mask is measured over a short time period, hence inducing an average power constraint. The choice of constraint has a significant impact on the choice of the number frames per bit, which is a critical parameter when considering reference-based systems. Hints of this dependence can be seen in the differing comparisons of [7], where FSR-UWB has shown to have optimality properties, for

a large number of frames and [9], where CM-UWB was shown to significantly outperform FSR-UWB for a small number of frames.

Per above, peak constraints are pertinent, and as described in [5], systems with a higher peak-to-average power ratio (PAPR) will need a higher number of frames and thus will need to be able to tolerate even more significant inter-frame interference (IFI). But the inability to tolerate arbitrary IFI puts a limitation on the number of frames. Therefore, strategies need to be considered to reduce the PAPR of many systems. Here, we employ a tone reservation tactic similar to that from orthogonal frequency division multiplexing (OFDM), where additional peak reduction carriers are used to alleviate the PAPR of the transmitted signal. But we hasten to emphasize that, unlike OFDM, these additional waveforms come at no cost in data rate. In particular, the constraint on the data rate for a multi-differential reference-based system is that the frequency offset of each data carrier from the reference must be less than the coherence frequency of the channel. But this constraint does not apply to the additional tones added for peak reduction. We demonstrate that the peak-reducing tones are still effective when placed at larger separations from the reference than the data carrying tones, and thus do not cause any appreciable loss in data rate.

The remainder of this chapter is organized as follows. Section 2.2 introduces the system model. Section 2.3 provides the development and performance analysis for the unified framework. Section 2.4 introduces peak mitigation techniques and Section 2.5 gives the numerical results for the reference-based systems considered. Finally, Section 2.6 provides the conclusions.

2.2 System Model

Throughout this Chapter, a baseband UWB system will be assumed. Since low data rate applications are targeted, a symbol interval $T_s = N_f T_f$ consists of

$N_f \gg 1$ frames, each of duration T_f and containing a single UWB pulse $p(t)$ with normalized energy $\int p^2(t)dt = 1/N_f$. Thus, for a given symbol interval, a data-carrying signal is modulated onto the unit-energy train of impulses $u(t) = \sum_{k=0}^{N_f-1} p(t - kT_f)$. In a general reference-based framework with K data-carriers, the transmitted signal consists of a reference signal and a collection of data signals, modulating the impulse train; hence, over the l^{th} symbol period, the transmitted signal is given by:

$$x(t) = u(t - lT_s)x_{env}(t - lT_s)$$

where

$$x_{env}(t) = \left(\sqrt{E_r} + \sum_{k=0}^{K-1} (-1)^{b_l^{(k)}} \sqrt{E_d^{(k)}} \phi_k(t) \right) \tag{2.1}$$

E_r and $E_d^{(k)}, k = 0, 1, ..., K-1$, represent the energy in the reference and k^{th} data-bearing signal respectively, $b_l^{(k)}$ is the k^{th} data bit in the l^{th} symbol period, and $\{\phi_k(t), k = 0, 1, \ldots, K-1\}$ is an orthogonal set of waveforms with normalization $\int_0^{T_s} \phi_k^2(t)dt = T_s$ for all k. Although it is not strictly necessary, we assume $\int_0^{T_s} \phi_k(t)dt = 0$ for all k, which is true of all of the major systems that have been introduced. The natural receiver is then given in Fig. 2.1, where $\tilde{r}(t)$ is the received signal, $r(t)$ is the low pass version of $\tilde{r}(t)$, and $r_l^{(k)}$ is the decision statistic that is thresholded to make a decision on the k^{th} bit sent during the l^{th} symbol period.

The original FSR-UWB [5] transmitted signal over interval $[lT_s, (l+1)T_s]$ is given by:

$$x_{fsr}(t) = \sqrt{E_r} u(t - lT_s) + (-1)^{b_l^{(k)}} \sqrt{2E_d} \cos(2\pi f_0 t) u(t - lT_s) \tag{2.2}$$

where $\sqrt{2}\cos(2\pi f_0 t)$ represents the waveform separating the reference and data waveforms, and $f_0 = 1/(2T_s)$ [28]. Note that FSR-UWB readily fits into the general

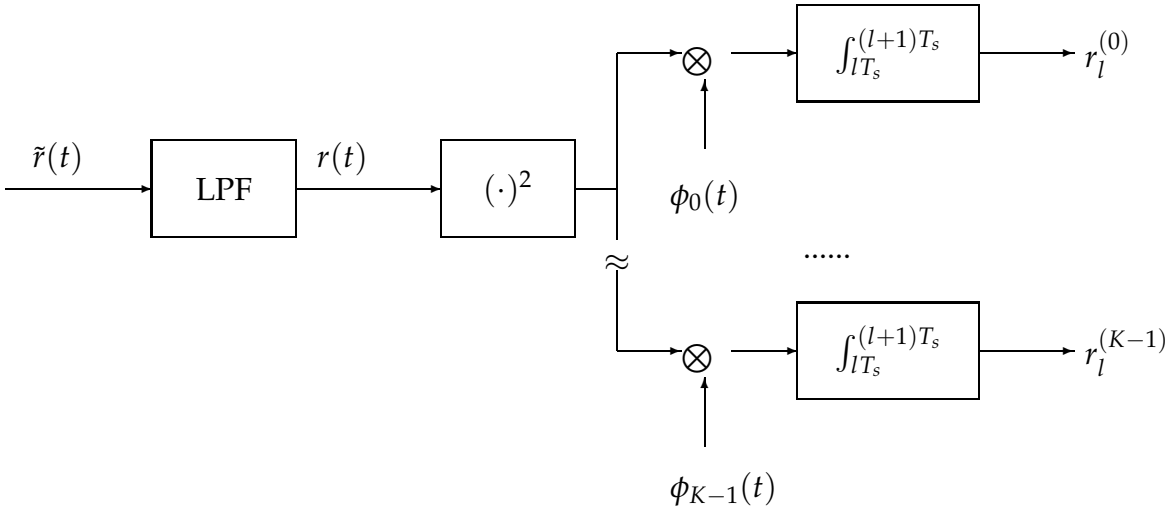


Figure 2.1: Natural receiver structure of a K-dimensional class of reference-based systems given in (2.1).

framework (2.1) with $K = 1$ and $\phi_0(t) = \cos(2\pi f_0 t)$. For multi-differential (MD-FSR-UWB), [34] where multiple sinusoidal are used in parallel as data carrying signals with a single reference, a critical constraint is that the frequency separation between the reference signal and most distant data carrier must lie below the coherence frequency of the channel so that the reference sounds the proper channel for all of the data carriers. This puts a constraint on the maximum combined data rate of the MD-FSR-UWB system. The transmitted signal on $[lT_s, (l+1)T_s]$, which readily fits the form of (2.1), is given by:

$$x_{MD-FSR}(t) = \sqrt{E_r}u(t - lT_s) + \sum_{k=0}^{K-1}(-1)^{b_l^{(k)}}\sqrt{2E_d^{(k)}}\cos(2\pi f_k t)u(t - lT_s) \qquad (2.3)$$

where K is the number of sinusoidal carriers, $f_0, f_1, \cdots, f_{K-1}$ are set by $f_k = (2k+1)f_0$ to ensure that interference among carriers does not fall at one of the frequency offsets of the data carriers from the reference.

Motivated by FSR-UWB, code shifted reference (CSR-UWB) [8] and code multiplexed (CM-UWB) [9] systems were developed. In CSR-UWB and CM-UWB, the orthogonality of reference and data pulses is obtained from the rows of a

Hadamard matrix. These codes yield square waves which form an orthogonal set. The transmitted signal in the baseline case is:

$$x_{CSR/CM}(t) = \sum_{m=0}^{N_f-1} p(t - mT_f) + (-1)^{b_0} \sum_{m=0}^{N_f-1} c_m p(t - mT_f) \tag{2.4}$$

where $\{c_m : m = 0, 1, ..., N_{f-1}\}$ represents a code sequence such that $c_m \in \{-1, +1\}$ for all m and $\sum_{m=0}^{N_f-1} c_m = 0$. This system fits into (2.1) with $K = 1$ and separating waveform:

$$\phi_0(t) = (-1)^{b_0} \sum_{m=0}^{N_f-1} c_m P_{T_f}(t - mT_f), \tag{2.5}$$

where

$$P_{T_f}(t) = \begin{cases} 1, & 0 \leq t \leq T_f \\ 0, & \text{otherwise.} \end{cases} \tag{2.6}$$

Clearly there are a large class of systems that fit into the reference based system framework in (2.1), since there are an uncountable number of sets of separating waveforms not yet considered. We unite the systems discussed thus far in addition to the large class of systems into a unified framework of reference based systems for joint analysis and design.

2.3 Performance Analysis

In this section, we consider the performance of an arbitrary system in the class.

2.3.1 Noiseless Case

First consider the output of the receiver of Fig. 2.1 in the noiseless case (i.e., $r(t) = x(t)$) for data bit $b_0^{(k)}$, where the first symbol (i.e., $l = 0$) is considered without loss of generality:

$$
\begin{aligned}
r_0^{(k)} &= \int_0^{T_s} x^2(t)\phi_k(t)dt \\
&= \int_0^{T_s} [\sqrt{E_r}u(t) + \sum_{m=0}^{K-1}(-1)^{b_0^{(m)}}\sqrt{E_d^{(m)}}\phi_m(t)u(t)]^2\phi_k(t)dt \\
&= \int_0^{T_s} u^2(t)[E_r\phi_k(t) + 2\sum_{m=0}^{K-1}(-1)^{b_0^{(m)}}\sqrt{E_rE_d^{(m)}}\phi_m(t)\phi_k(t) \\
&\quad + \sum_{m=0}^{K-1}\sum_{n=0}^{K-1}(-1)^{b_0^{(m)}}(-1)^{b_0^{(n)}}\sqrt{E_d^{(m)}E_d^{(n)}}\phi_m(t)\phi_n(t)\phi_k(t)]dt \qquad (2.7) \\
&\approx \frac{E_r}{T_s}\int_0^{T_s}\phi_k(t) + \frac{2\sqrt{E_rE_d^{(k)}}}{T_s}(-1)^{b_0^{(m)}}\int_0^{T_s}\phi_k^2(t)dt \qquad (2.8)
\end{aligned}
$$

Note that there will be many integrals of the form $\int_0^{T_s} u^2(t)g(t)dt$, where $g(t)$ is a narrowband signal. The result of this integral is approximately $\frac{1}{T_s}\int_0^{T_s} g(t)dt$ because the narrowband signal $g(t)$ can be approximated constant over an interval T_p and the number of frames is large [5]. Clearly, the second of the remaining two terms in (2.7) is the desired term, and, in contrast to [7], we see that there are significant constraints on the set $\phi_k(t), k = 0, 1, ..., K-1$ to make the third term vanish. One way to state the constraint is that the product of any two separating waveforms in the set must have zero inner product with any other separating waveform. As expected, the more specific version of this constraint has been obtained in each of the MD-FSR case [34] and the CSR case [8]. With this constraint on the separating waveforms,

$$
r_0^{(k)} \approx 2\sqrt{E_rE_d^{(k)}}(-1)^{b_0^{(m)}} \qquad (2.9)
$$

As in [5], maximization of the useful receiver output in the noiseless case can be used for energy allocation because the "noise cross noise" term dominate at error rates of interest. From the convexity of the bit error rate on a given data carrier K as a function of the energy $E_d^{(k)}$, it is clear that $E_d^{(0)} = E_d^{(1)} = ... = E_d^{(K-1)}$ at the optimal point. Hence we need to maximize $E_rE_d^{(k)}$ subject to $KE_d^{(k)} + E_r = E_s$.

The maximum is achieved by setting $E_r = \sum_{k=0}^{K-1} E_d^{(k)} = \frac{E_s}{2}$, and $E_d^{(k)} = \frac{E_s}{2K}$; hence, $r_0^{(k)} = \frac{E_s}{\sqrt{K}}(-1)^{b_0^{(k)}}$.

2.3.2 Performance in Additive White Gaussian Noise (AWGN) Channels

The received signal is given by $\tilde{r}(t) = x(t) + \tilde{n}(t)$, where $\tilde{n}(t)$ is a zero-mean Gaussian random process with (two-sided) power spectral density (PSD) of $N_0/2$. Assuming the lowpass filter at the receiver front end passes the transmitted signal without distortion, its output signal is given by $r(t) = x(t) + n(t)$, where $n(t)$ is a zero-mean Gaussian random process with PSD $|H(f)|^2 N_0/2$ and $H(f)$ is the frequency response of the lowpass filter. For the k^{th} bit of symbol $l = 0$, the integrator outputs are:

$$\begin{aligned} r_0^{(k)} &= \int_0^{T_s} r^2(t)\phi_k(t)dt \\ &= \int_0^{T_s} [x(t) + n(t)]^2 \phi_k(t)dt \\ &\approx \frac{E_s}{\sqrt{K}}(-1)^{b_0^{(k)}} + 2\int_0^{T_s} x(t)n(t)\phi_k(t)dt + \int_0^{T_s} n^2(t)\phi_k(t)dt \end{aligned} \tag{2.10}$$

The latter two terms, which will be denoted the "noise terms", will be grouped into a single random variable n_0. Following the argument in [4, 5], we assume that n_0 is approximately Gaussian. Hence, only its mean and variance are required to characterize system performance. The mean of n_0 is given by:

$$\begin{aligned} E[n_0] &= 2\int_0^{T_s} E[x(t)]E[n(t)]\phi_k(t)dt + \int_0^{T_s} E[n^2(t)]\phi_k(t)dt \\ &= \sqrt{2}\int_0^{T_s} R_n(0)\phi_k(t)dt \\ &= 0 \end{aligned} \tag{2.11}$$

where $R_n()$ denotes the autocorrelation function of $n(t)$, and the variance of n_0 is given by:

$$
\begin{aligned}
E[n_0^2] &= E[(2\int_0^{T_s} x(t)n(t)\phi_k(t)dt + \int_0^{T_s} n^2(t)\phi_k(t))^2] \\
&= E[(2\int_0^{T_s} x(t)n(t)\phi_k(t)dt)^2] + E[(\int_0^{T_s} n^2(t)\phi_k(t))^2] \qquad (2.12) \\
&= 2E_rN_0 + \frac{2N_0}{T_s}\int_0^{T_s}\sum_{m=0}^{K-1} E_d^{(m)}\phi_m^2(t)\phi_k^2(t)dt \\
&\quad + \frac{2N_0}{T_s}\int_0^{T_s}\sum_{m=0}^{K-1}\sum_{n\neq m}^{K-1}(-1)^{b_0^{(m)}}(-1)^{b_0^{(n)}}\sqrt{E_d^{(m)}E_d^{(n)}}\phi_m(t)\phi_n(t)\phi_k^2(t)dt \\
&\quad + T_sN_0^2W \qquad (2.13)
\end{aligned}
$$

where the last line comes from a similar analysis done in [5]. For simplicity in further sections we will refer to the "signal cross noise" term by SCN, defined below, and derived in Appendix A.

$$
\begin{aligned}
SCN \triangleq\ & \frac{2N_0}{T_s}\int_0^{T_s}\sum_{m=0}^{K-1} E_d^{(m)}\phi_m^2(t)\phi_k^2(t)dt \\
& + \frac{2N_0}{T_s}\int_0^{T_s}\sum_{m=0}^{K-1}\sum_{m\neq n}^{K-1}(-1)^{b_0^{(m)}}(-1)^{b_0^{(n)}}\sqrt{E_d^{(m)}E_d^{(n)}}\phi_m(t)\phi_n(t)\phi_k^2(t)dt \qquad (2.14)
\end{aligned}
$$

Following the definition from above, the bit error probability in the general framework is :

$$
P_b = Q\left(\frac{E_s\sqrt{K}}{\sqrt{T_sN_0^2W + SCN}}\right) = Q\left(\frac{E_b\sqrt{K}}{\sqrt{T_sN_0^2W + SCN}}\right) \qquad (2.15)
$$

A similar error performance is observe at practical error rates across all systems that employ the same K, since the "noise cross noise" term dominates at the (high) uncoded error rates of interest. Comparisons are reserved for a later section.

2.3.3 Multipath Fading Channels

For a multipath fading channel, the received signal is:

$$
\tilde{r}(t) = h(t) * x(t) + \tilde{n}(t) \qquad (2.16)
$$

where $h(t)$ is the system impulse response, which is assumed to consist of L discrete paths, and thus can be represented as:

$$h(t) = \sum_{l=0}^{L-1} h_l \delta(t - \tau_l), \tag{2.17}$$

where $\delta(\cdot)$ is the Dirac delta function, and τ_l and h_l are the delay and amplitude of the l^{th} path, respectively. Again, because the "noise cross noise" term dominates at the (high) error rates of interest in uncoded systems [7], the key is the noiseless decision statistic:

$$\begin{aligned}
r_0^{(k)} &= \int_0^{T_s} (\sum_{l=0}^{L-1} h_l x(t-\tau_l))^2 \phi_k(t) dt \\
&= \sum_{l=0}^{L-1} \sum_{m=0}^{L-1} h_l h_m \int_0^{T_s} x(t-\tau_l) x(t-\tau_m) \phi_k(t) dt \\
&= \sum_{l=0}^{L-1} \sum_{m=0}^{L-1} h_l h_m \int_0^{T_s} u(t-\tau_l) u(t-\tau_m) \left(\sqrt{\frac{E_s}{2}} + \sum_{k=0}^{K-1} (-1)^{b_0^{(k)}} \sqrt{\frac{E_s}{2K}} \phi_k(t-\tau_l) \right) \\
&\quad \left(\sqrt{\frac{E_s}{2}} + \sum_{n=0}^{K-1} (-1)^{b_0^{(n)}} \sqrt{\frac{E_s}{2K}} \phi_n(t-\tau_m) \right) \phi_k(t) dt \\
&= \frac{E_s}{2\sqrt{K}} \sum_{l=0}^{L-1} \sum_{m=0}^{L-1} h_l h_m \int_0^{T_s} \left(\sqrt{K} + \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} \sum_{n=0}^{K-1} (-1)^{b_0^{(k)}} (-1)^{b_0^{(n)}} \right. \\
&\quad \left. \phi_k(t-\tau_l) \phi_n(t-\tau_m) + \sum_{k=0}^{K-1} (-1)^{b_0^{(k)}} \phi_k(t-\tau_l) + \sum_{n=0}^{K-1} (-1)^{b_0^{(n)}} \phi_n(t-\tau_m) \right) \\
&\quad u(t-\tau_l) u(t-\tau_m) \phi_k(t) dt \\
&\approx (-1)^{b_0^{(k)}} \frac{E_s}{\sqrt{K}} \sum_{l=0}^{L-1} h_l^2 \frac{1}{T_s} \int_0^{T_s} \phi_k(t-\tau_l) \phi_k(t) dt \\
&+ (-1)^{b_0^{(k)}} \frac{E_s}{2\sqrt{K}} \sum_{l=0}^{L-1} \sum_{l \neq m} h_l h_m \frac{1}{T_s} \int_0^{T_s} \left(\phi_k(t-\tau_l) + \phi_k(t-\tau_m) \right) \phi_k(t) dt \rho(|\tau_l - \tau_m|)
\end{aligned} \tag{2.18}$$

where $\rho(.)$ gives the normalized energy in the (often zero or partial) overlap of UWB pulses of the separation of its argument; that is,

$$\rho \triangleq N_f \int_0^{T_f} p(t - (\tau \mod T_f))p(t)dt \tag{2.19}$$

The motivation of the derivation above is to investigate what properties of $\phi_k(t)$ will impact performance. Therefore, following [7], we define the autocorrelation function of $\phi_k(t)$ as:

$$R_{\phi_k}(\tau) = \frac{1}{T_s} \int_0^{T_s} \phi_k(t)\phi_k(t-\tau)dt \tag{2.20}$$

Substituting (2.20) into (2.18) yields:

$$r_0^{(k)} = (-1)^{b_0^{(k)}} \left(\frac{E_s}{\sqrt{K}} \sum_{l=0}^{L-1} h_l^2 R_{\phi_k}(\tau) + \frac{E_s}{2\sqrt{K}} \sum_{l=0}^{L-1} \sum_{l \neq m} h_l h_m R_{\phi_k}(\tau_l) R_{\phi_k}(\tau_m) \rho(|\tau_l - \tau_m|) \right) \tag{2.21}$$

The first summand in (2.21) is generally positive for systems of interest, whereas the second summand can often be negative due to the mismatch in the signs of the path gains h_l and h_m. This suggests, maximizing the first summand, which would indicate a large $R_{\phi_k}(\tau)$ for $\tau \in [0, \tau_{max}]$ [7] corresponding to a broad autocorrelation function. But minimizing the second term would suggest a small $R_{\phi_k}(\tau)$ corresponding to a narrow autocorrelation function. This gives conflicting results on the optimal settings for $\phi_k(t)$ to be considered later.

2.4 Peak Reduction via Tone Reservation

In the extensions of FSR-UWB and CM-UWB, and, for other systems with $K > 1$, a high PAPR might be encountered. Therefore, to make reference-based systems feasible in the multi-data case, techniques need to be investigated that can contribute to reducing the overall PAPR of the system. The peak reduction solution considered here is similar to the tone reservation technique used in OFDM [37]. In this method, additional carriers are employed to carry signals that minimize the overall peak of the transmitted signal. These carriers do not affect signal detection at the receiver because they are orthogonal to the data carriers. The key insight

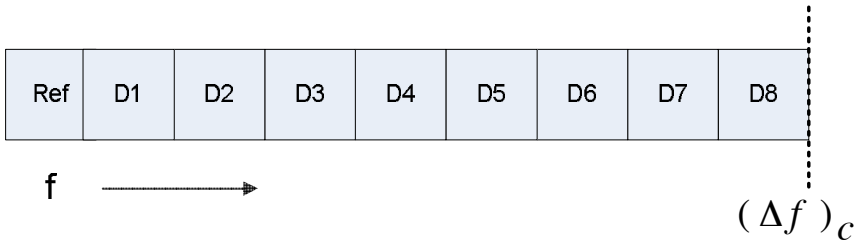
here is that, since these peak reducers need not necessarily be interleaved with the data carriers, they can be placed at frequency offsets greater than that of the data carriers and above the coherence bandwidth of the system. In particular, recall that data carriers need to be at frequency offsets below the coherence bandwidth so that the reference properly sounds the channel. By placing the peak reduction tones at higher frequency offsets, the data rate of the system is not affected, as shown in Fig. 2.2. The transmit signal now becomes:

$$\begin{aligned} x(t) &= \sqrt{E_r}u(t-lT_s) + \sum_{k=0}^{K-1}(-1)^{b_l^{(k)}}\sqrt{E_d^{(k)}}u(t-lT_s)\phi_k(t-lT_s) \\ &\quad + \sum_{p=0}^{P-1} m_p u(t-lT_s)\phi_{K+p}(t-lT_s) \end{aligned} \tag{2.22}$$

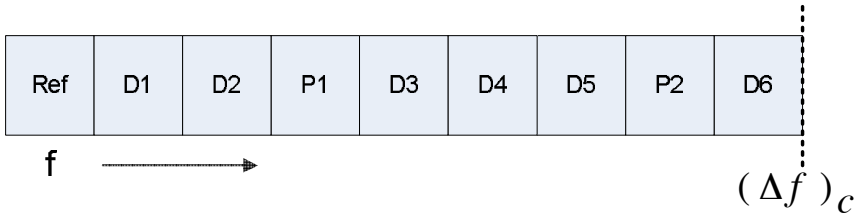
where P is the number of peak reduction waveforms. Here, the amplitudes of these extra waveforms, $m_p, p = 0, 1, ..., P-1$, are chosen optimally via a convex optimization so that the peak power of the signal $x(t)$ is minimized. In practice, this optimization would be done off-line for each possible set of data bits and the results stored in a table for efficient on-line usage.

In choosing the number of these carriers, P, there are a few issues to consider. First, the average energy of the transmitted signal needs to be carefully observed, since it gets larger by adding these carriers. Although the system must pay a total average power penalty to accommodate the extra waveforms, a system that is IFI-limited will not be able to increase N_f to deal with PAPR problems (see [5]), and thus the reduction of the absolute peak allows more average energy to be put into the data carriers. Secondly, N_f should be large enough to prevent the extra carriers from effectively getting aliased to lower frequency tones.

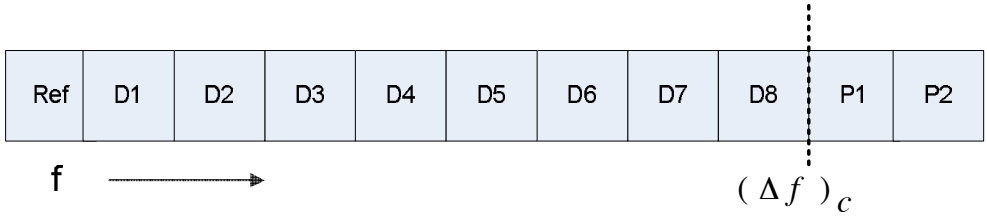
A simple example is given in Fig. 2.3 for the envelope of the signal $x(t)$ given in (2.22). For a given P, optimal coefficients, m_p's, can be found to minimize the peak value of the resulting signal. Clearly, the peak value decreases with increas-



(a) Original MD-FSR system with data carriers D1, D2,… D8.



(b) MD-FSR system with interleaved peak reduction tones P1 and P2 (P=2). Note the reduction in data rate.



(c) MD-FSR system with peak reduction tones at end (P=2). Note the data rate is the same as in (a).

Figure 2.2: An example illustrating the difference of interleaving versus placing peak reducing tones at the end for peak reduction

ing number of carriers and approaches to a limit, which is the value as $P \to \infty$. Knowing this limit reveals how close a given system is to the optimum achievable. It is difficult to find this limit directly as it involves optimizing countably infinite coefficients. Hence, we employ a dual space technique.

As in (2.1), let

$$x_{\text{env}}(t) = \sqrt{E_r} + \sum_{k=0}^{K-1} (-1)^{b_l^{(k)}} \sqrt{E_d^{(k)}} \phi_k(t - lT_s) + \sum_{p=0}^{P-1} m_p \phi_{K+p}(t - lT_s)$$

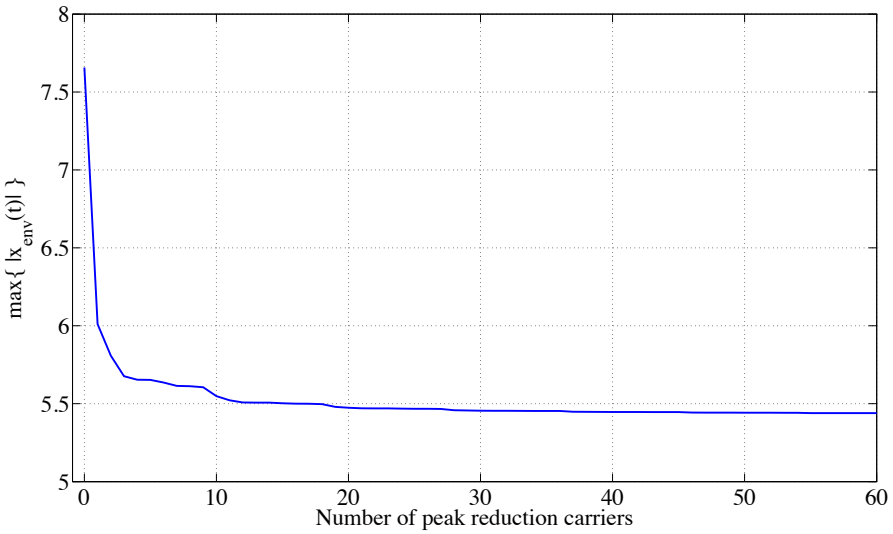


Figure 2.3: Peak value of the envelope of an MD-FSR signal as a function of the number of peak reduction carriers. For the example signal, $K = 4, E_r = 4, E_d^{(k)} = 1, b^{(k)} = 1, \forall k$. The original peak value is $2 + 4\sqrt{2}$. The peak value of the signal decreases with increasing P and approaches a limit.

be the envelope of the MD-FSR signal which modulates the pulse train. Let $x_{\text{ref}}(t)$, $x_{\text{data}}(t)$ be the part of this signal that carries the reference and the data, respectively, and $m(t) = \sum_{p=0}^{\infty} m_p \phi_{K+p}(t - lT_s)$ be the signal added for peak reduction. With these definitions,

$$x_{\text{env}}(t) = x_{\text{ref}}(t) + x_{\text{data}}(t) + m(t) \tag{2.23}$$

is the signal which is required to have minimal peak value. Note that the peak value of a signal is its infinity norm, denoted by $\|\cdot\|_\infty$ and notice that

$$\|x_{\text{ref}}(t) + x_{\text{data}}(t) + m(t)\|_\infty = \|x_{\text{data}}(t) + m(t)\|_\infty + \sqrt{E_r}. \tag{2.24}$$

Then, the peak minimization problem can be equivalently posed as

$$\text{minimize} \quad \|x_{\text{data}}(t) + m(t)\|_\infty . \tag{2.25}$$

The requirement here is that $m(t)$ is a linear combination of functions in the set $\{\phi_k(t), k = K, K+1, \cdots\}$, which is a set of orthogonal functions. Thus, the minimum peak value is

$$\min_{m(t)\in \text{span}\{\phi_k(t), k=K,K+1,\cdots\}} \|x_{\text{data}}(t) + m(t)\|_\infty + \sqrt{E_r}. \tag{2.26}$$

To find this value, we make use of the following theorem:

Theorem 1 ([38, pg. 119]) *Let M be a subspace in a real normed space X. Let X^* be the dual space of X. Then,*

$$\min_{\boldsymbol{m}\in M^\perp \subset X^*} \|\boldsymbol{x} + \boldsymbol{m}\| = \sup_{\boldsymbol{y}\in M\subset X,\ \|\boldsymbol{y}\|\leq 1} < \boldsymbol{y}, \boldsymbol{x} > . \tag{2.27}$$

For $\mathbf{y} \in X$ and $\mathbf{x} \in X^*$, $< \mathbf{y}, \mathbf{x} >$ denotes the result of the functional when $\mathbf{x}$ *acts upon* $\mathbf{y}$. The vector that maximizes the value $< \mathbf{y}, \mathbf{x} >$, $\mathbf{y}_{\text{opt}}$, lies in the subspace M, while the vector $\mathbf{m}_{\text{opt}}$ lies in the space $M^\perp$. $M^\perp$ is defined as the set of vectors which result in zero when applied on any vector in M. The peak reduction problem in (2.26) is a problem in the space L^∞. Thus, we find the minimum peak value by solving the corresponding (easier) maximization problem in the space L^1 which has its dual L^∞. In other words,

$$\min_{m(t)\in M^\perp \subset L^\infty} \|x_{\text{data}}(t) + m(t)\|_\infty = \sup_{y(t)\in M\subset L^1,\ \|y(t)\|_1\leq 1} < y(t), x_{\text{data}}(t) > . \tag{2.28}$$

Here, $m_{\text{opt}}(t)$ lies in the subspace $M^\perp = \text{span}\{\phi_k(t), k = K, K+1, \cdots\}$. In MD-FSR, $\phi_k(t) = \cos(2\pi(2k+1)f_0 t)$, hence

$$M = \text{span}\Big\{ \{\cos(2\pi(2k+1)f_0 t), k = 0, 1, \cdots, K-1\} \cup \{\sin(2\pi k f_0 t), k = 1, 2\cdots\} \\ \cup \{\cos(2\pi(2k)f_0 t), k = 0, 1, 2\cdots\} \Big\}$$

Within this subspace M, finding $y_{\text{opt}}(t)$ is not easier than finding $m_{\text{opt}}(t)$. However, we narrow down the subspace M by the following observations:

1. Projection of $y_{\text{opt}}(t)$ onto span$\{\sin(2\pi k f_0 t), k = 1, 2 \cdots\}$ is the zero signal, because $< \sin(2\pi k f_0 t), x_{\text{data}}(t) >= 0, \forall k$, and adding a sine function to $y(t)$ only increases the 1-norm.

2. Projection of $y_{\text{opt}}(t)$ onto span$\{\cos(2\pi(2k) f_0 t), k = 0, 1, 2 \cdots\}\}$ is the zero signal, because $< \cos(2\pi(2k) f_0 t), x_{\text{data}}(t) >= 0, \forall k$, and adding an even frequency cosine function to $y(t)$ only increases the 1-norm.

Hence, the subspace that $y_{\text{opt}}(t)$ lies is confined to span$\{\cos(2\pi(2k+1) f_0 t), k = 0, \cdots, K-1\}$. Thus $y(t) = \sum_{k=0}^{K-1} y_k \cos(2\pi(2k+1) f_0 t)$, where y_k's are real scalars to be optimized. Then,

$$< y(t), x_{\text{data}}(t) >= \sum_{k=0}^{K-1} (-1)^{b_l^{(k)}} \sqrt{E_d^{(k)}} y_k, \tag{2.29}$$

which results in the following optimization problem:

$$\text{maximize} \quad \sum_{k=0}^{K-1} (-1)^{b_l^{(k)}} \sqrt{E_d^{(k)}} y_k \tag{2.30}$$

$$\text{subject to} \quad \int_0^{T_s} \left| \sum_{k=0}^{K-1} y_k \cos(2\pi(2k+1) f_0 t) \right| dt \leq 1. \tag{2.31}$$

This K-parameter maximization problem (e.g., $K = 4$ in Fig. 2.3) is clearly easier to solve than the norm minimization problem with countably infinite parameters in the dual space. The result of this maximization problem plus $\sqrt{E_r}$ is equal to the minimum peak value that can be achieved. Numerical results are given in the next Section.

2.5 Numerical Results

Per above, the constraints under which the system comparison is made are critical, as can be evidenced by the conflicting results of [7] and [9]. Here we consider both peak and average power constraints.

For all the results presented, the pulse shape is the second derivative Gaussian with a zero-to-zero pulse width of .25 ns. The noise bandwidth, corresponding to that of a front end filter, is 4.0 GHz (one-sided). Simulation results were conducted over multipath channels from the IEEE 802.15.4a standardization [2]. The two channels considered were IEEE 802.15.4a indoor line-of-sight (LOS) model (CM3) and IEEE 802.15.4a indoor non-light-of-sight (NLOS) model (CM4).

2.5.1 Average Power Constraint (Small N_f Case)

With solely an average power constraint, system performance is optimized ([35, 36]) by employing a small number of frames (N_f) per symbol. In [9] significant performance differences have been observed between CSR/CM-UWB and FSR-UWB for small N_f which, for a fixed frame period, corresponds to large data rates. Here we probe this comparison further. When IFI is not considered, FSR suffers degradation because its modulating $x_{env}(t)$ is not constant over a frame period. Therefore one possible solution would be to sample the envelope at the beginning of each frame and hold that sample across the frame period, hence making it constant over the frame period. This sample-hold approach will be called "modified FSR-UWB" (M-FSR-UWB). Furthermore, as investigated in detail in [5], the frequency offset causes a performance degradation as the data rate approaches the coherence frequency of the channel. In [28], it is noted that the frequency offset of FSR-UWB can be halved to address this latter concern. This alternative to the original FSR-UWB is "FSR-2-UWB" where instead of the frequency offset $f_0 = \frac{1}{T_s}$, an offset of $f_0 = \frac{1}{2T_s}$ is used to enhance system performance.

In Figs. 2.4, 2.5 performance is considered under an average power constraint, which corresponds to small N_f, as described above. For the high data rate of 7.8 Mbps ($N_f = 8$) FSR-UWB has poor performance compared to the other systems considered. M-FSR-UWB shows improved performance compared to FSR, FSR-2-UWB shows slightly better performance compared to CSR-UWB.

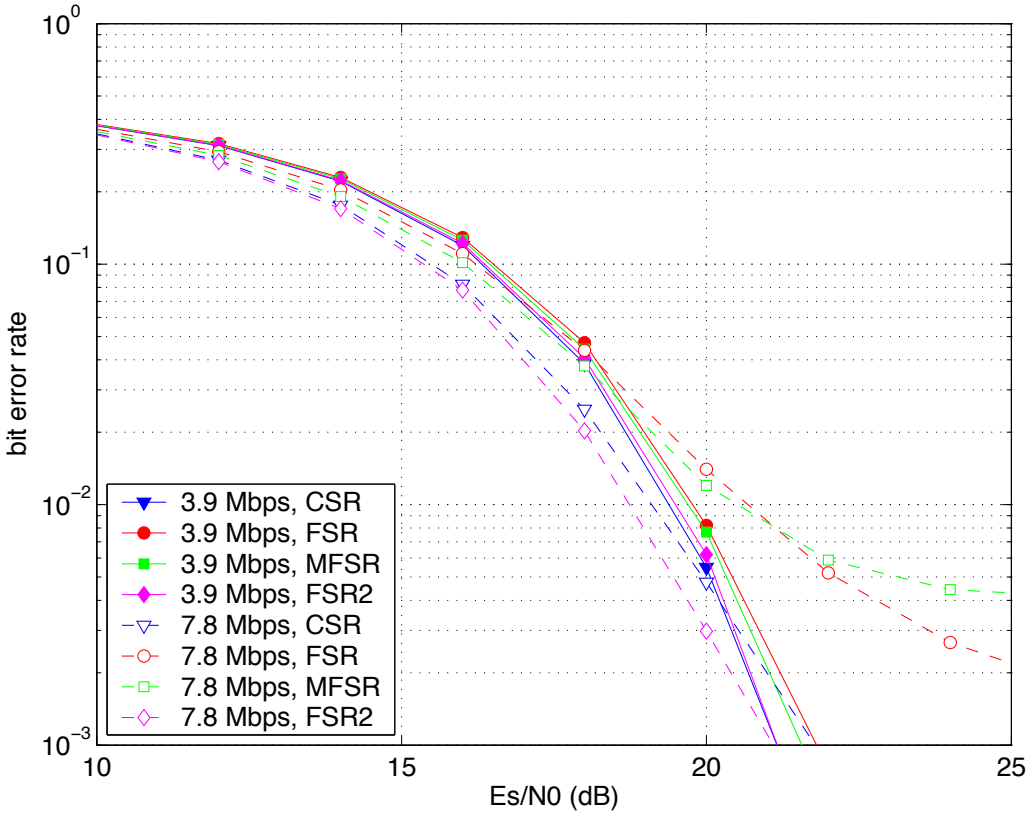


Figure 2.4: Simulated results for the performance of various binary schemes on the IEEE 802.15.4a indoor LOS model (CM3) with a fixed frame time of T_f = 16 ns, N_f = 8 (dashed curves) and N_f = 16 (solid curves) which correspond to R_b = 7.8 Mbps and 3.9 Mbps, respectively. For each point, 10^6 data symbols have been simulated.

2.5.2 Peak Power Constraint (Large N_f Case)

CMOS technology trends shows that there will be peak-power limitations in low-power-integrated circuitry for an ultra-wideband transmitter, as described in [10]. For devices to meet the circuit constraints, FCC spectral mask, and maximize

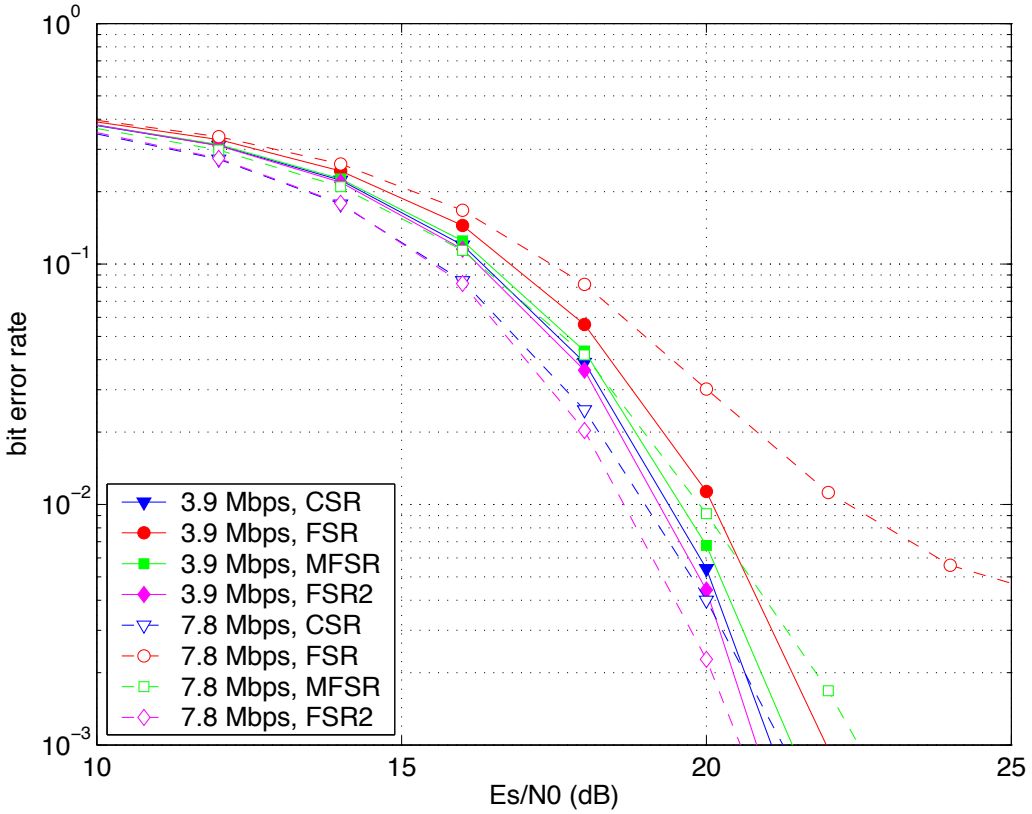


Figure 2.5: Simulated results for the performance of various binary schemes on the IEEE 802.15.4a indoor NLOS model (CM4) with a fixed frame time of T_f = 16 ns, N_f = 8 (dashed curves) and N_f = 16 (solid curves) which correspond to R_b = 7.8 Mbps and 3.9 Mbps, respectively. For each point, 10^6 data symbols have been simulated.

system performance from a commercialization perspective under a peak power constraint would suggest large N_f (on the order of approximately 75 pulses, in [10]). This is further exacerbated in systems with significant PAPR, because they must further increase N_f to boost average power [5].

For large N_f, our analysis and [7] suggest a broad autocorrelation function $R_{\phi_k}(\tau)$ of the separating waveform would correspond with improved system performance. In the case of binary CM-UWB, as considered in [9], the optimal separating waveform would be

$$\phi(t) = \begin{cases} 1 & 0 \leq t \leq \frac{1}{2} \\ -1 & \frac{1}{2} < t \leq 1 \\ 0 & \text{otherwise} \end{cases} \tag{2.32}$$

which corresponds to the burst-mode PPM, and is arrived at through a different derivation in [9].

In Figs. 2.6, 2.7 we consider performance under a peak power constraint which corresponds to a large N_f. We see that systems underneath this constraint again have similar performance, and thus for the binary case, conclude that ease of implementation is the key differentiator. This points to CM/CSR-UWB approaches, which avoid not only the delay lines of TR-UWB but also the amplitude modulation of FSR-UWB.

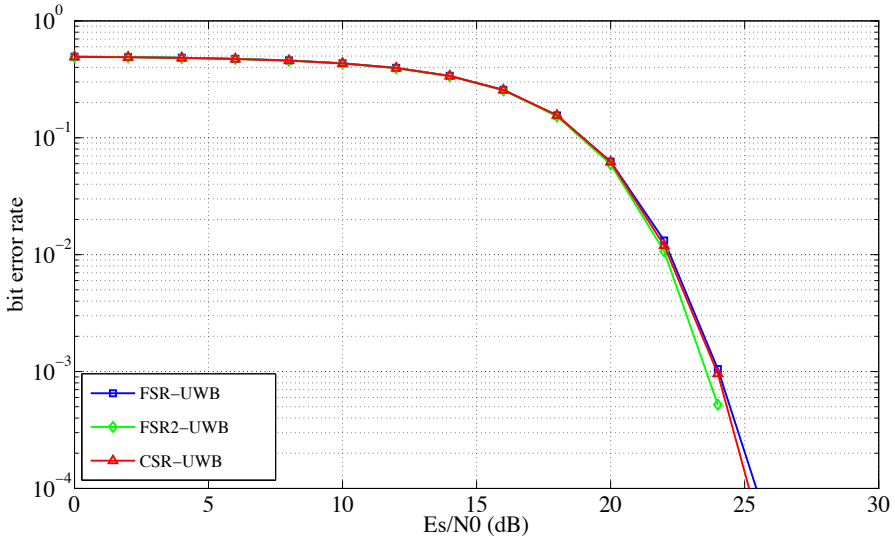


Figure 2.6: Simulated results for the performance of various binary schemes on the IEEE 802.15.4a indoor LOS model (CM3) with a fixed frame time of T_f = 15.5 ns, N_f = 64 which correspond to R_b = 1 Mbps. For each point, 10^6 data symbols have been simulated.

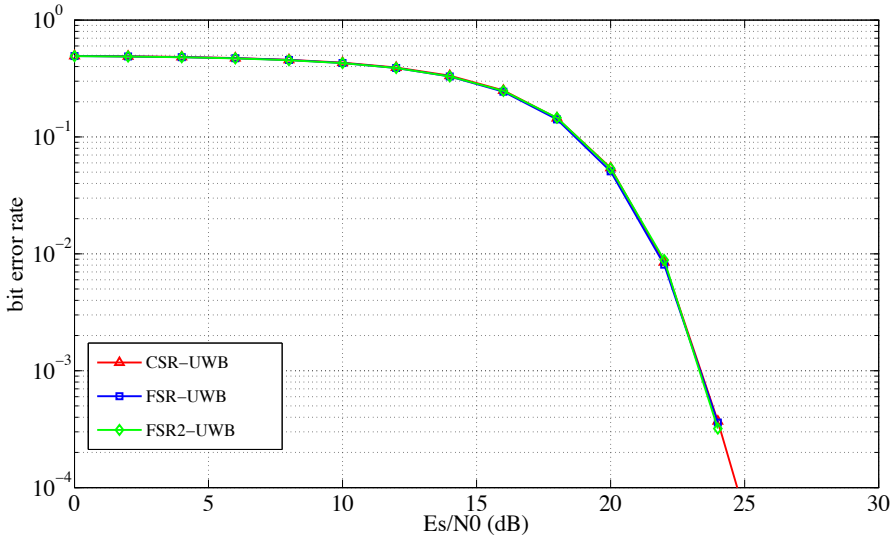


Figure 2.7: Simulated results for the performance of various binary schemes on the IEEE 802.15.4a indoor NLOS model (CM4) with a fixed frame time of T_f = 15.625 ns, N_f = 64 which correspond to R_b = 1 Mbps, respectively. For each point, 10^6 data symbols have been simulated.

2.5.3 Peak Reduction via Tone Reservation

Per above, performance can be greatly improved versus the binary systems by employing more data carriers; however, PAPR problems must be addressed. One approach is peak reduction via tone reservation (Section 2.4) where the PAPR value of the transmitted signal is reduced with no change in the receiver system and without compromising in bit error rate performance. In Fig. 2.8 the simulated bit error rate performance of an MD-FSR system with and without peak reduction is compared. As expected, for all three channels simulated, bit error rates remain the same under both cases for all SNR values. This supports the claim that adding orthogonal carriers to the transmitted signal does not affect the detection performance. Next, how the number of peak reduction carriers, P, affects the amount of peak reduction is considered. Of course, P can be increased to achieve smaller peaks and this increase will have no effect on the bit error rate performance. However, the increased number of carriers give diminishing gains and

	initial peak $(max\|x_{env}(t)\|)$	initial and final energy	peak reduction (dB)	final peak
FSR, $K = 4$	0.8263	1, 1.7487	2.9270	0.5899
CSR/CM, $K = 4$	0.6475	1, 1	0	0.6475
FSR, $K = 2$	0.6475	1, 1.3185	2.1436	0.5059
CSR/CM, $K = 2$	0.5211	1, 1	0	0.5211
FSR, $K = 1$	0.5211	1, 1.0978	1.1605	0.4559
CSR/CM, $K = 1$	0.4317	1, 1	0	0.4317

Table 2.1: Peak reduction results for CSR/CM-UWB and FSR-UWB schemes (N_f = 128, T_f = 31.25 ns, and P = 20)

there is a nonzero limit to how much the peak can be reduced, as considered in Section 2.4. The change of peak reduction as a function of the number of extra carriers is shown in Fig. 2.9. In this example, peak reducing carriers are placed at higher frequencies than the data carriers. We further explore how peak minimization is improved when the frequencies of the data and peak reduction carriers are selected optimally (possibly by interleaving their frequency locations). In Fig. 2.9, it can be seen that relocating the frequencies does not return much in terms of peak reduction. So we conclude that peak reduction is not significantly below optimal when the peak reduction carriers are placed at higher frequency offsets than the data carriers. It might also seem possible to add extra carriers to a CSR/CM-UWB signal for peak reduction. However, while a CSR/CM-UWB signal has a lower initial peak compared to FSR-UWB, the specific separating waveforms used in CSR/CM-UWB do not allow peak reduction by adding extra carriers. Table 2.1 presents the peak values before and after peak reduction for CSR/CM-UWB and FSR-UWB for the case of $K = 1, 2, 4$ carriers and $P = 20$ peak reducers.

2.6 Conclusion

We have considered the comparison of recently proposed reference-based systems under both peak and average constraints. Including all of these systems into a single framework allows for a unified performance analysis and suggests optimality properties to guide system design. For reference-based systems with a

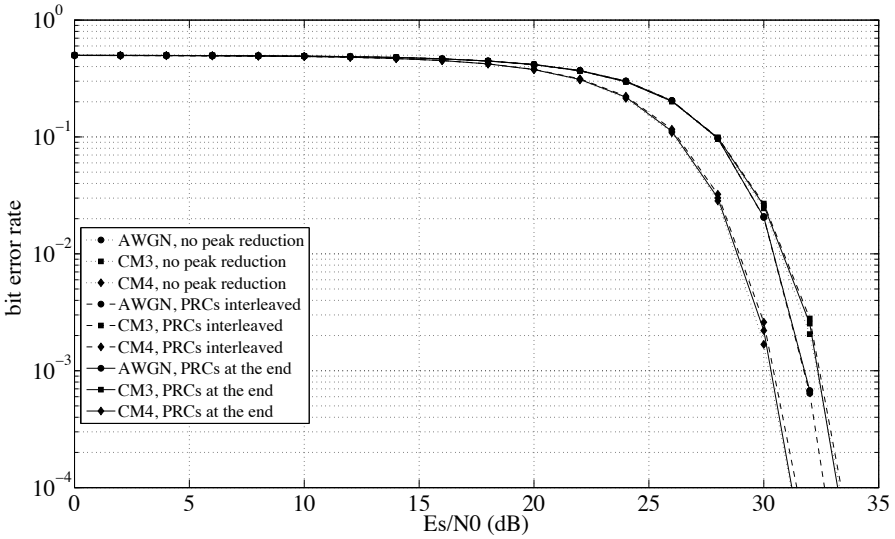


Figure 2.8: BER computed for an MD-FSR system with 5 data carriers for different SNR values. Three different channels are simulated for cases (1) without peak reduction and (2) with peak reduction by adding 3 extra carriers. As expected, for all the three channels simulated, bit error rates remain the same under both cases for all SNR values. This justifies the fact that adding orthogonal carriers to the transmitted signal do not affect the detection performance.

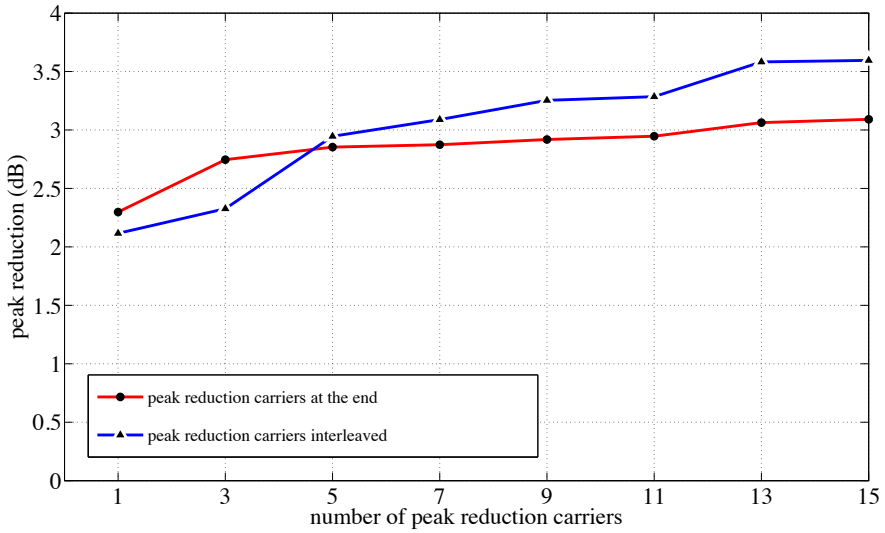


Figure 2.9: Peak Reduction of Multi-Differential FSR-UWB with additional tones (K=5), while either interleaved in blue with triangle markers or at the end in red with circle markers.

single data carrier, halving the frequency offset between reference and data in the frequency-shifted reference UWB system, as suggested in recent work, leads to slight performance advantages over alternatives under peak and average power constraints. However, since the gains are slight, this suggest code-multiplexed or code-shifted reference UWB systems for implementation, since they avoid the amplitude modulation required in the frequency-shifted reference UWB system. In the binary case, the optimal code-multiplexed and code-shifted reference UWB systems reduce to burst-mode pulse-position modulation, which is akin to what has been employed in the 802.15.4a standard.

Systems that employ multiple data carriers with a single reference have the potential to greatly improve performance versus their single data carrier counterparts; however, all considered systems then require amplitude modulation, and can suffer from a significant PAPR, which limits performance under peak power constraints. Here, we have introduced peak mitigation alternatives that do not restrict the data rate and are effective for some systems in the class, most notably for the multiple data carrier version of frequency-shifted reference UWB. Such peak mitigation techniques lead to small PAPR gains of frequency-shifted reference UWB versus code-multiplexed and code-shifted reference UWB systems.

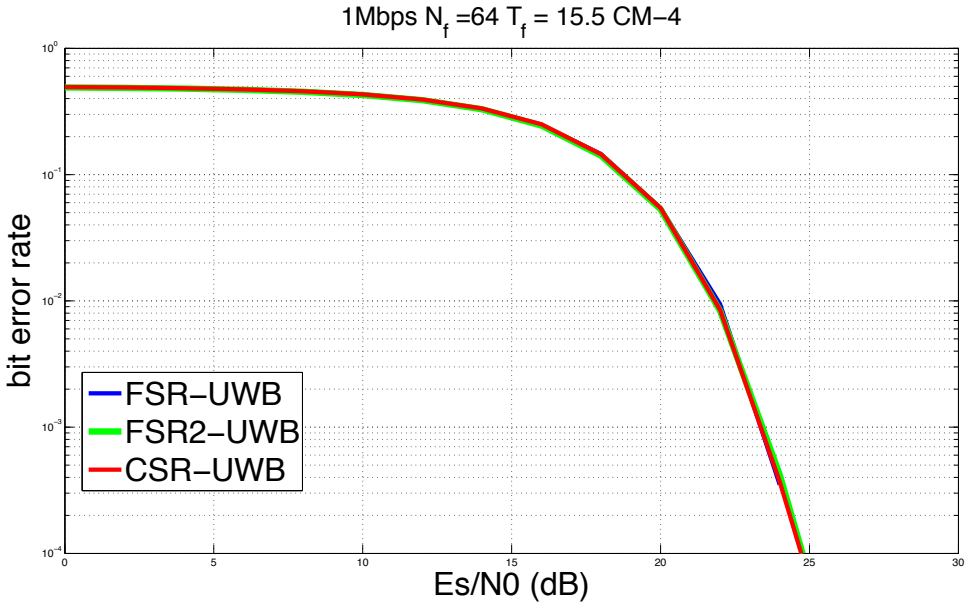


Figure 2.10: Performance of various binary schemes on the IEEE 802.15.4a indoor NLOS model (CM4) with a fixed frame time of $T_f = 15.5$ ns, $N_f = 64$ ($R_b = 1$ Mbps).

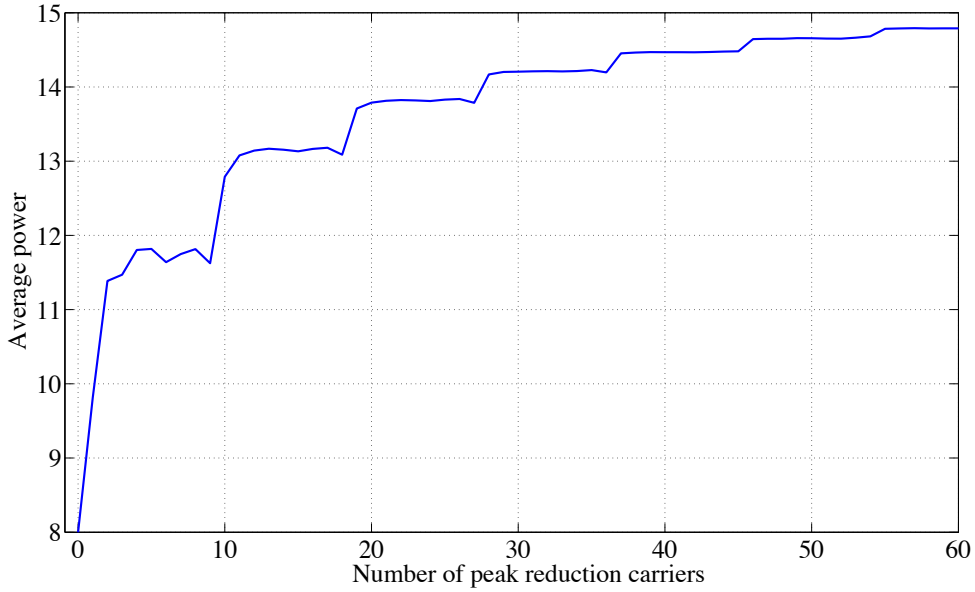


Figure 2.11: Average power of the MD-FSR signal as a function of the number of peak reduction carriers, P. As P increases, the peak value of the signal goes down (see Fig. 2.3) and the average power increases.

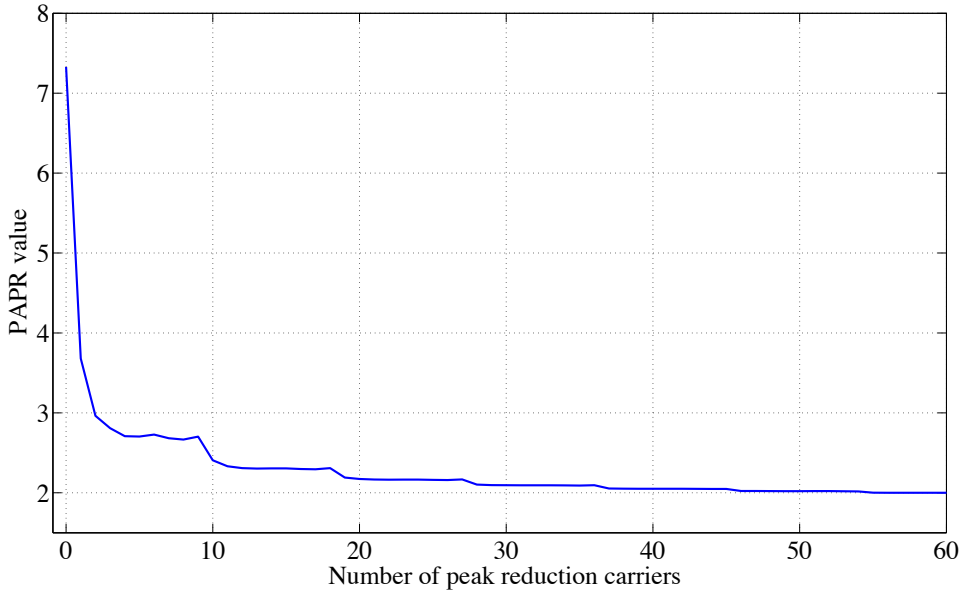


Figure 2.12: Peak to average power (PAPR) of the MD-FSR signal as a function of the number of peak reduction carriers, P. As P increases, the peak value of the signal goes down (see Fig. 2.3) while the average power increases (see Fig. 2.11), hence PAPR value decreases.

CHAPTER 3

WIRELESS SECURITY: SECRECY RATE PAIR CONSTRAINTS FOR SECURE THROUGHPUT

Physical layer security, which is an alternative to traditional crytpographic methods, has emerged as a promising candidate to protect wireless transmissions from an eavesdropper. An important measure of physical layer security is the secrecy outage: the event when the instantaneous secrecy capacity, which for the considered scenario is the difference between the capacity of the Alice (the transmitter) to Bob (the legitimate receiver) channel and the capacity of the Alice to Eve (the eavesdropper) channel, is below a target secrecy rate for which the system has been designed. In this Chapter, we argue that design under such an outage definition on a wireless channel is inadequate in some scenarios, as it treats very different error events with equal weight. In response, we propose that two conditions are met: the instantaneous capacity between the source and destination is above a target rate and the instantaneous capacity between the source and eavesdropper is held below a target rate. The two individual target rates form a secrecy rate pair. This also naturally splits the outage event into two regions with quite different costs: the eavesdropper's ability to decode the message (which is a security breach and must be avoided), and the destination's inability to decode the message (which simply requires a re-transmission). We use our formulation to consider rate pair selection in hybrid ARQ systems and provide numerical results supporting this approach. At the end of the Chapter we extend these results to the two-hop network, where optimization is done numerically.

3.1 Background

Many organizations and companies are focusing significant energy and resources on security because of the negative consequences of an insecure network (e.g. identity theft, secret intel). In the next sections we will give background on cryptographic security and then focus on information-theoretic security for the remainder of the dissertation.

3.1.1 Cryptographic Security

Cryptography has been a standard way to secure wireless (or any) communications: modify the transmitted signal in such a way that a user with the cryptographic key can easily decode the signal, whereas a user without the key is thwarted by their inability to solve a "hard" problem with current computational resources. The technique of using a shared secret key is known as symmetric encryption. Symmetric encryption relies heavily on the ability to establish a shared secret key, which can be very difficult to do in large networks. A weakness of this system is that it is susceptible to a key possibly falling into the hands of the eavesdropper. In contrast asymmetrical encryption employs a public key encryption system. Asymmetrical encryption systems allow users to establish security over a public channel without both users sharing the same private key. A commonly use example of asymmetric encryption in cryptography is shown in Fig. 3.1, the widely used DiffieHellman key exchange protocol [21], where the source and destination establish a key over an insecure channel. The eavesdropper is at a significant computational disadvantage to decode the message because he/she does not know the secret integers chosen by the source and destination. For example consider this simplistic example of the Diffie-Hellman key exchange protocol:

1. Alice and Bob agree on two prime numbers p, g, where g is a primitive root modulo p. In practice this is 512 bits but for simplicity we will consider the case when $p = 7, g = 3$.

2. Alice and Bob choose secretly known random integers a and b respectively, privately known to them only. Alice sends $A = g^a \mod p$ and Bob sends $B = g^b \mod p$. For the case of Alice and Bob choosing $a = 8, b = 15$ results in $A = 2, B = 6$.

3. Alice and Bob compute their shared secret key S, which is equal to $B^a \mod p = 1, A^b \mod p = 1$.

In this cryptosystem Alice and Bob now share the secret key S (in the above example $S = 1$), while $p, g, g^a \mod p, g^b \mod p$ are public. The Diffie-Hellman algorithm highlights a strong assumption typically seen in cryptography: limited computational abilities of the eavesdropper.

There have been many cryptogrphaic techniques which have become obsolete and ineffective at security because of flaws seen later on. A widely known example is 802.11b wired equivalent privacy (WEP) encryption that was shown insecure [39] because the length of the key is 24 bits, which meant a key was reused every 16 million frames, making it very vulnerable to a brute force attack in a quick time interval. Another problem with WEP was that it lacked true randomness and thus keys were closely related. Lastly, a hardware issue was that an important part of the Initial Vector (IV) frame, always reset to 0 on power cycle.

Currently, the field of quantum computing is a primary candidate to challenge current computational resource assumptions. Projects such as "Penetrating Hard Targets" and "Owning the Net" are projects invested into quantum research, attempting to decrypt some of the most widely used encryption algorithms such as Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) [40] . RSA was first pub-

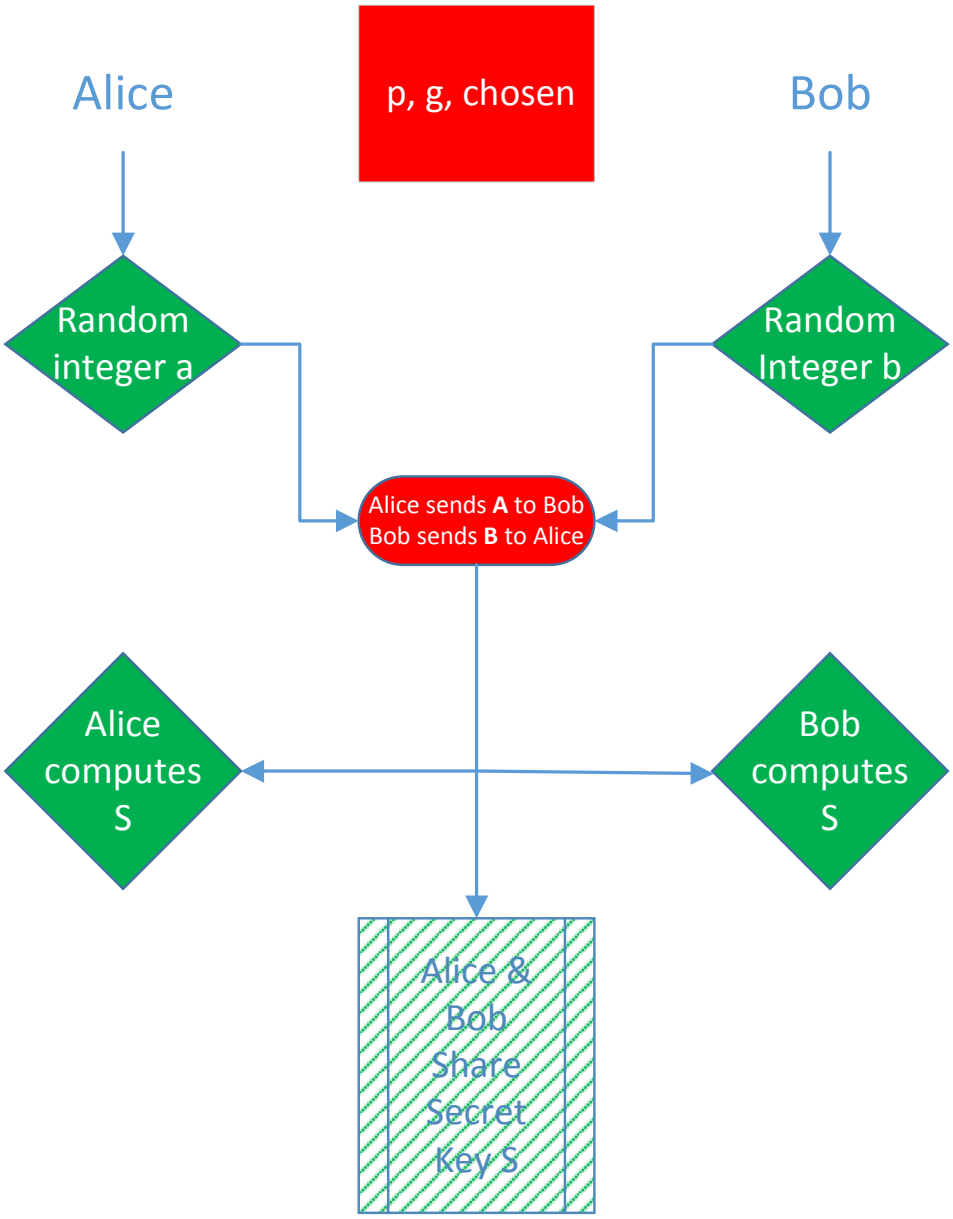


Figure 3.1: Simplified flow diagram of the Diffie-Hellman public key exchange protocol. The green shaded boxes represent information that is privately known to Alice or Bob (secret key S, integers a, b). The red shaded rectangular boxes represent public information (p, g, A, B).

lished in 1977, a public-key asymmetrical cryptosystem where the encoding key is public and the decryption key is private. The complexity and hardness of RSA

comes from the difficulty in factoring the product of two large prime numbers (prime factorization problem).

In general three central drawbacks of cryptography can be summarized as:

Assume limited computational resources of an eavesdropper, which can be challenged as new forms of computation is considered. First, there exist no unbreakable cryptographic encryption schemes. In early 2009 it was shown using a group of classical computers and methods that a 768 bit key could be cracked (although it took over 2 years to accomplish). Most companies use a 1024-bit encryption key, which is estimated to take over 100 times longer to crack. However, quantum research advances could be the downfall of traditional cryptographic techniques.

They are based on the assumption of hardness of the underlying primitives which has not been proven. When information-theoretic security cannot be achieved, cryptographers seek an alternative using computational security. Cryptographers assume adversaries are computationally limited, but the hardness of a problem is difficult to prove. Problems which suggest hardness include integer factorization, where for large numbers no efficient factorization algorithm is known as in the widely used RSA algorithm, and the discrete logarithm problem, solving the equation $b^k = g$ for k, where no efficient algorithmic solution is known (e.g. Diffie-Hellman key exchange). Computational security proofs are not valid though, only if these problems that are believed to be hard are indeed so ($P \neq NP$); in other words, they cannot be solved in polynomial time.

The message can be stored by an eavesdropper for later decoding after obtaining the key, hence breaking the cryptographic system. Very important is that this translates to not having everlasting security, although many forms of information

are to sensitive forever or for a long time. For example in World War II, in the Venona project [41] (1941-1946), the Soviet Union used two-time pads (which will be discussed in more detail in the following section), which were insecure since message bits were leaked to the U.S.A. and Britain. The Allies were able to leverage this flaw to decode some of the messages.

3.1.2 Wireless Environment

Thus far we have discussed cryptographic (computational) security which in summary relies on the limited computational abilities of an eavesdropper to solve a "hard problem" given current computational resources. But computational security does not need to take advantage of the natural disruptions ubiquitous in the physical (wireless) environment. In particular the wireless environment experiences especially path loss and fading. Path loss is the degradation of the signal amplitude with distance as it travels through the medium, and fading is multiple copies of the signal traveling a different path experiencing attenuation, phase shift and delay. As a result if the signal has to travel a long distance, one can expect detection to be more difficult than a signal that travels a shorter distance. Information-theoretic physical layer security, which will be formally introduced in the next section, takes full advantage of the noisy wireless environment and does not rely on computational assumptions on the eavesdropper, thus providing everlasting security immune from cryptanalyst techniques. Information-theoretic security cannot be obtained when there is no advantage to exploit in the wireless environment, e.g. the eavesdropper is very close to the source. In contrast because cryptography ignores the wireless environment, it is unaffected by the position of an eavesdropper.

3.1.3 Information-theoretic Security

In contrast to cryptography, information-theoretic physical layer security has recently emerged as a method to secure wireless links irrespective of the current or future computational capabilities of the eavesdropper. In short, the signal the eavesdropper observes does not contain enough information to identify the transmitted message. Moreover this assumption is different than cryptography, where message contents are widely available though in an encrypted form. Information-theoretic security was pioneered by Claude Shannon in his seminal work in [22]. Information-theoretic security does not rely on a key but an advantage on the channel, guarantees everlasting security: no contents of the message are leaked to Eve and the message is secure forever.

Shannon first considered physical layer security for a noiseless wireline channel. Shannon modeled the following scenario (Fig. 3.2): Alice (source) desires to communicate secretly to Bob (destination) in the presence of Eve (eavesdropper), and Alice has a secure link with Bob where they share K information bits, also known as the key. Shannon, mathematically, defined the notion of information-theoretic secure as the mutual information between the message M and the encoding function $X(g_K(M))$ as nil:

$$I(M;X) = H(M) - H(M|X) \tag{3.1}$$

where $I(M;X)$ is the measure of uncertainty between the message and the encoding function, $H(M)$ is the measure of unpredictability in the message M and $H(M|X)$ represents the measure of uncertainty of the message M, given you know the encoding function X. If the above (3.1) is non-zero, then contents of the message are leaked to Eve. Shannon then proceeded to answer the following questions:

1. How long must K be for an N-bit message M?

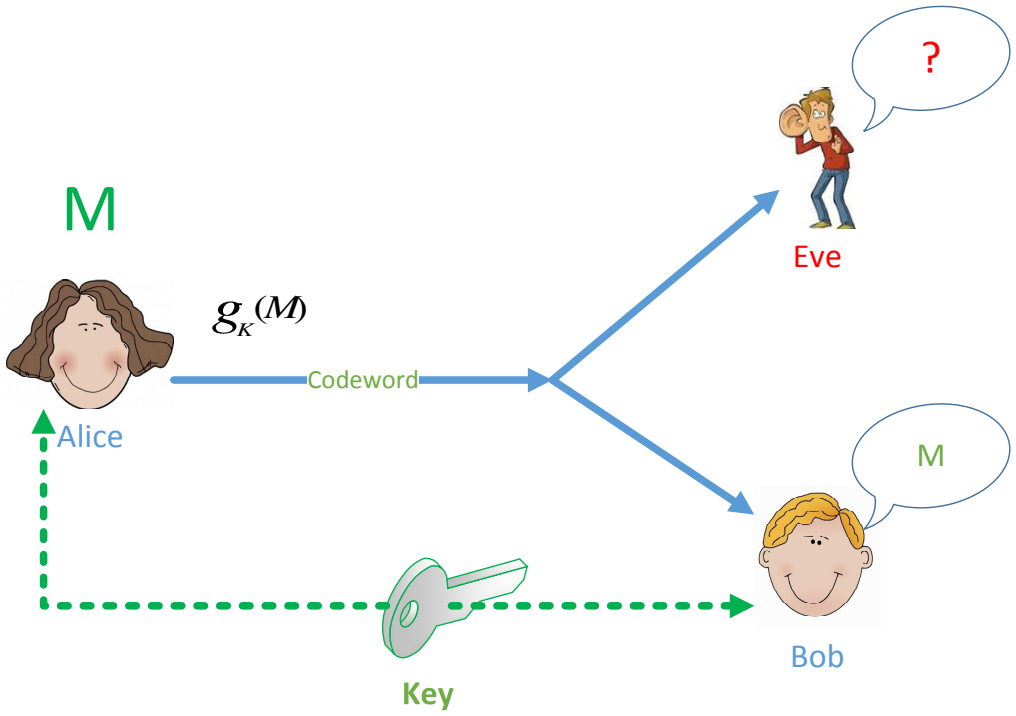


Figure 3.2: Wireline channel: Alice establishes a private secure link (green dashed line) with Bob so that they can establish a private shared key. Alice encodes the message with the private key to form a codeword to communicate to Bob. Eve is able to listen perfectly to the codeword, where $g_K(M)$ represents the encoding function, and M is the message. The goal is to ensure the eavesdropper is completely uncertain of the message (?) while the destination can reliably decode the message (M).

2. How do you choose $g_K(M)$?

For the first question he noted that, to guarantee secrecy, the key had to be as long as the message, and, for the latter question, concluded the encoding function to be the onetime pad [22]. As shown in Fig. 3.3, Bob is able to easily decode the message because of knowledge of the pre-shared key, whereas Eve receives a codeword which has little to no use without information about the key. We have considered unique keys, for each individual messages, but can we reuse keys which could lead to a more practical and efficient design? Consider the extension of the one-time pad to a two-time pad (Fig. 3.4). Unfortunately in this scenario, Eve

can derive $(M_1 \oplus K_1) \oplus (M_2 \oplus K_1) = M_1 \oplus M_2$. Although Eve does not directly have M_1 or M_2 exclusively, K information bits have been leaked; in this case, the scheme is not information-theoretic secure. This classic example was exploited in the Venona project during WW2. The U.S.A. was able to crack some of the Soviet Union's messages because of broken one-time pads that reuse keys (two-time pads), in which case the U.S.A was able to decode 20% of the coded messages [41].

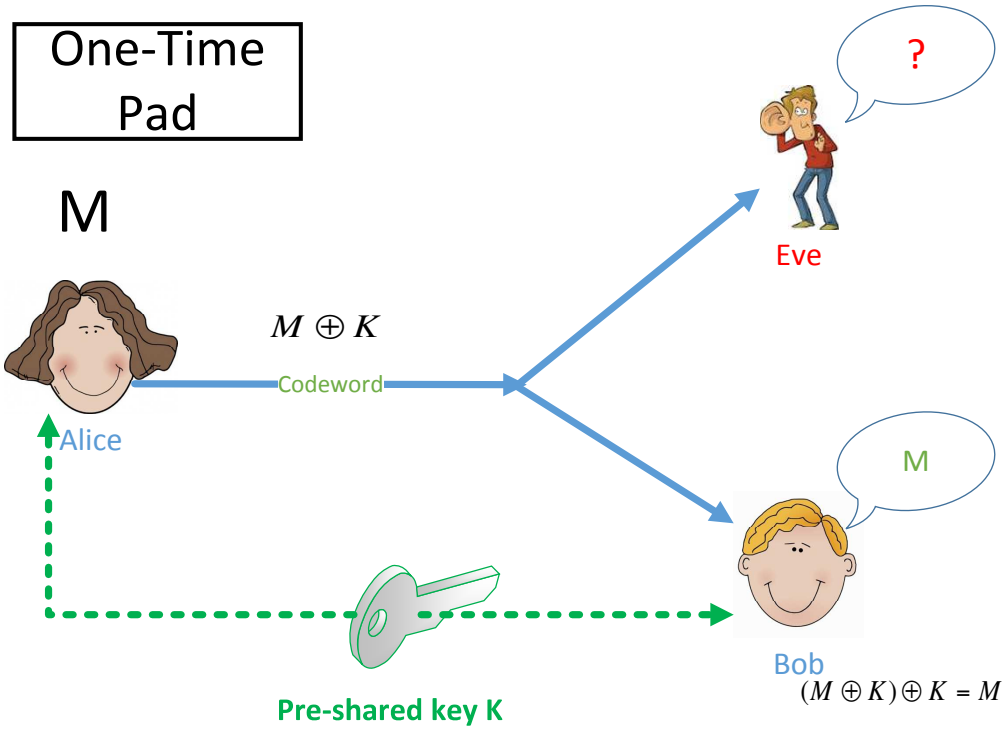


Figure 3.3: The one-time pad, which guarantees everlasting security, is shown. Alice takes each message (M) and xor's with a one-time key, because Alice-to-Bob has a secure link where they can establish a shared key about which Eve has no information. Perfect security is met and Alice can communicate securely to Bob.

3.2 Wiretap Channel

Following Shannon's work, Wyner considered secrecy over a noisy channel, the wiretap channel, where the signal observed at the eavesdropper is a degraded version of the signal observed at the legitimate receiver [13]. For this degraded

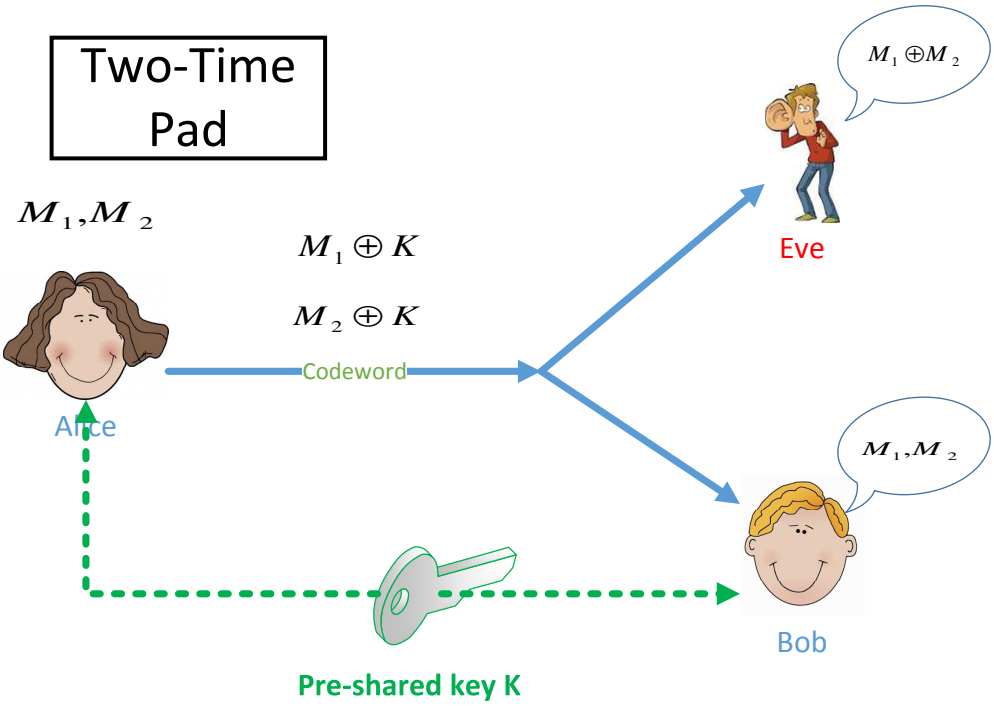


Figure 3.4: The two-time pad is an extension to the one-time pad, where instead the key is reused for multiple messages. This is insecure and dangerous because e.g. English has enough redundancy and ASCII encoding where the individual M_1 and M_2 can be easily extracted.

scenario, Wyner came to the conclusion that a non-zero information rate can be maintained by the transmitter and receiver while the eavesdropper gets no information about the message. Of interest for our work is the extension of this result to the Gaussian channel [42]. Further work has demonstrated that, under quite general conditions, the secrecy capacity is given by the difference in the capacities between the main channel and the eavesdropper channel [11, 23, 24].

3.2.1 Wiretap Construction

Wyner first noted the signal observed at the eavesdropper is a degraded version of the signal observed at the legitimate receiver; the wiretap channel [13]. Later, it was proven for the Gaussian channel that a non-zero information rate can be

maintained if the Alice to Eve channel is worse than the Alice to Bob channel [42]:

$$R = \log_2(1 + SNR_{AB}) - \log_2(1 + SNR_{AE}) \tag{3.2}$$

The main result is that for the wiretap channel, a positive secrecy rate can be achieved as long as the instantaneous secrecy rate is above the target secrecy rate. In practice and mathematical terms all Gaussian channels are degraded versions of each other; thus, Fig. 3.5 represents the mathematical model. Next, and perhaps most important are the construction of codes for the wiretap channel, which rely on answers to the following key questions:

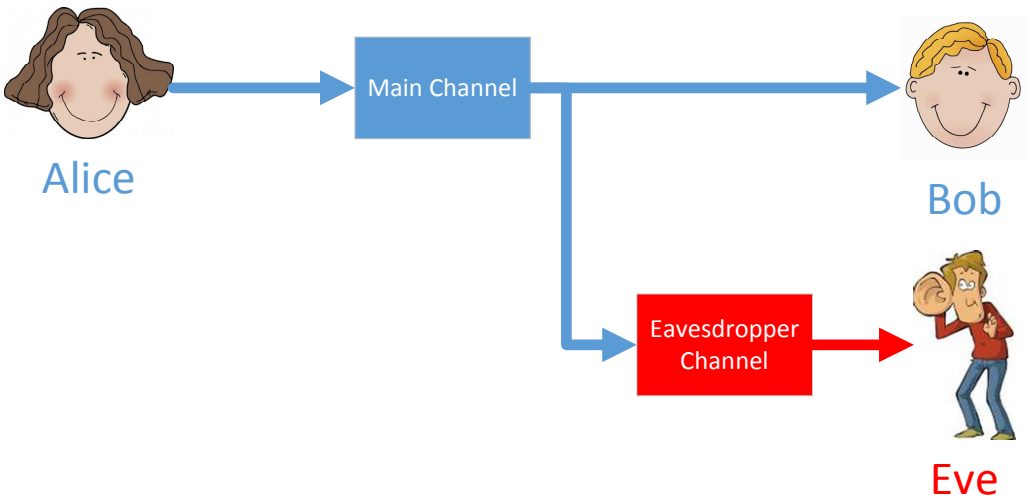


Figure 3.5: The wiretap channel is shown. Alice desires to communicate to Bob through the main channel. The eavesdropper listens to the message but through the degraded eavesdropper channel.

1. What is the maximum rate at which the Alice can communicate to Bob (main channel, R_{AB}) ?

2. What is the maximum rate in which Eve can listen to Alice (eavesdropper channel, R_{AE}) ?

As a result of this information, and dictated by the channel conditions, a target secrecy capacity can be calculated from the difference of the rates of the main and eavesdropper channel. Next, the code book construction is considered:

1. The source (Alice) generates $2^{NR_{AB}}$ random codewords.

2. Alice splits these codewords randomly into $2^{NR_{AE}}$ bins.

3. The codebook is broadcast to everyone.

This code construction maps $R_0 = R_{AB} - R_{AE}$ information bits to the appropriate bin. For simplicity, Fig. 3.6 depicts the wiretap code construction case when $N = 1$ (in practice N would be very large), $R_{AB} = 4, R_{AE} = 2$; therefore, $R_0 = 2$. In this example Alice first generates 16 random codewords; second, randomly splits these 16 codewords into 4 bins; and, last, broadcasts the codebook to everyone. For example, consider the case where Alice desires to send the information bits 11 to Bob. Alice would randomly select a bin and use the information bits as the least significant bits to identify a codeword in that bin as shown in Fig. 3.7. Bob is able to successfully decode the exact codeword, and the bin yields the message due to the fact Bob can receive at 4 bits, and accurately distinguish between the 16 codewords as seen in Fig. 3.8a. In contrast Eve is unable to decode the message because Eve receives at 2 bits; therefore Eve can only accurately produce a list of 4 possible codewords, which will produce 4 codewords which are randomly spread across the bin, as illustrated in Fig. 3.8b. Note that in a practical system where N is large the ambiguity at Eve is larger. We will show later that this natural interpretation of the wiretap code yields a different formulation than the standard formulation, which will be discussed in more detail in the next section.

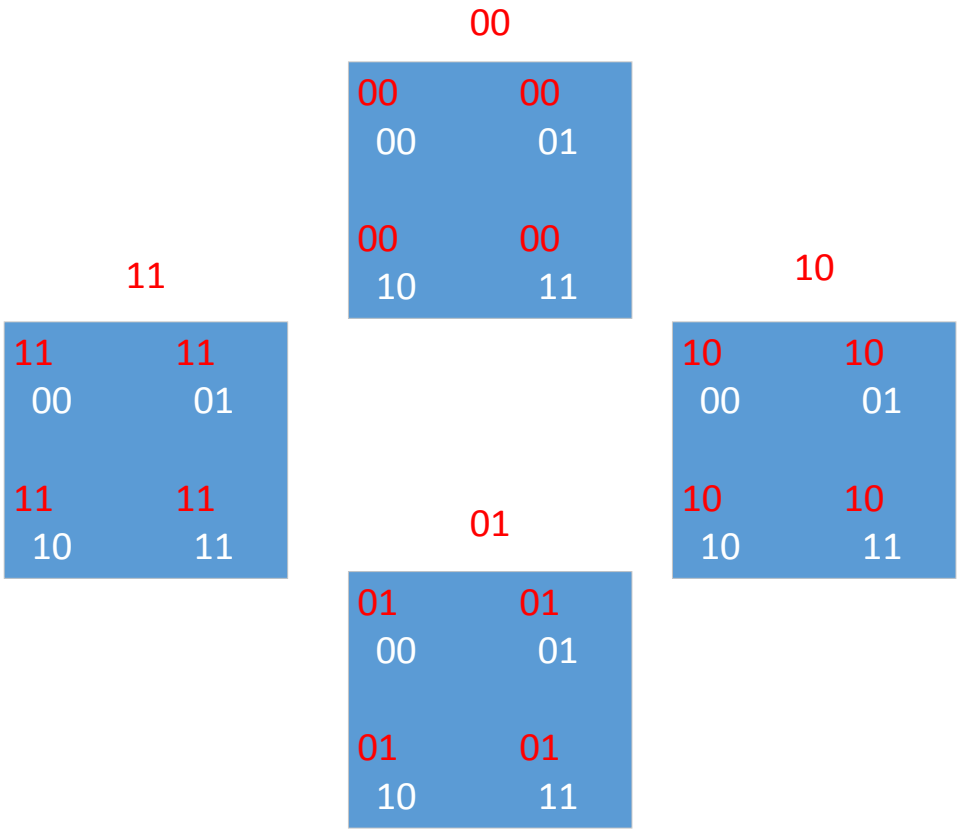


Figure 3.6: A cartoon ($N = 1$) example of the wiretap construction is shown for an instantaneous rate to Bob and Eve at 4 and 2 bits, respectively, that yields a secrecy rate of 2 bits. The 16 ($2^{R_{AB}}$) codewords and 4 ($2^{R_{AE}}$) bins represent the rate to Bob and Eve, respectively.

3.3 Secrecy Rate Pair Formulation

On wireless communication channels, the randomness of the fading gains makes it impossible to guarantee secrecy over every instantiation of the fading, hence motivating the concept of secrecy outage. The instantaneous capacity is defined as the maximum rate of information that can be reliably transmitted between Alice and Bob conditioned on the fading, noted as R_B; likewise, between Alice and Eve, R_E. The secrecy outage is generally defined as the probability the instantaneous secrecy capacity ($R_S = R_B - R_E$), the difference between the instantaneous capacity

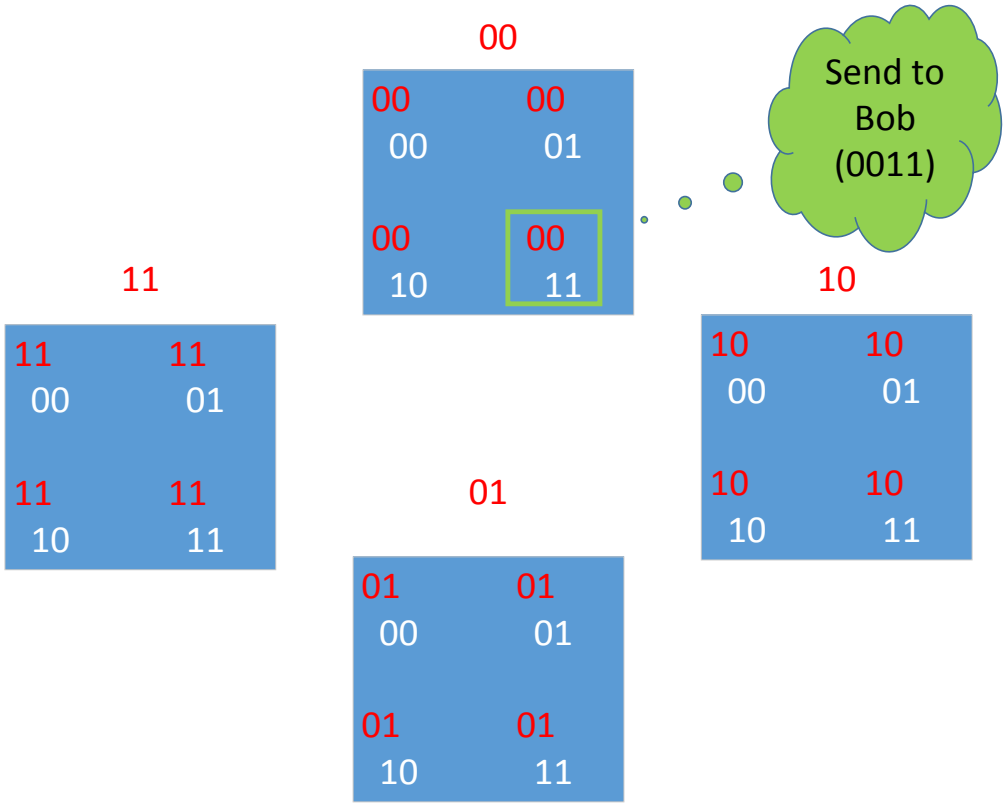
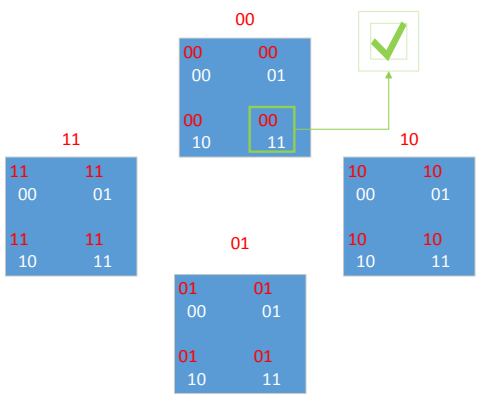


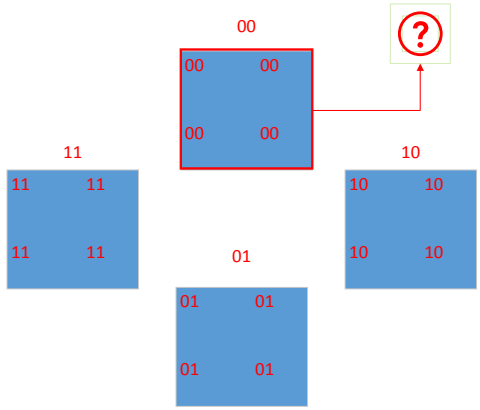
Figure 3.7: Alice desires to send bits 11 to Bob and randomly chooses bin 00 to send the message. The codeword sent is 0011 with the public bits 00.

of the Alice and Bob (R_B) channel and that of the Alice and Eve (R_E) channel, is less than the targeted secrecy rate (R_0) [11, 12]. Hence for a secure system, secrecy is achieved when the secrecy rate (R_S) is above the designed secrecy rate ($R_S \geq R_0$).

Figure 3.9 shows the secrecy region as a function of R_E and R_B when $R_0 = 2$. The target secrecy rate is $R_0 = 2$, and the entire shaded region represents $R_S = R_B - R_E \geq 2$, where channel conditions are favorable and the secrecy capacity is above the targeted secrecy rate. However, because "universal" wiretap codes are unknown, we maintain that it can be difficult to guarantee secrecy over the entire region where $R_S = R_B - R_E \geq 2$. For example, consider a wiretap code designed for the rate pair, $R_B = 4, R_E = 2$ which we will denote as $R_S(4,2)$. Consider channel conditions which maintain the secrecy rate constraint ($R_S \geq 2$) but where



(a) Bob receives at a rate of 4 bits, determines that the codeword is 0011 and extracts the information bits 11.



(b) Eve receives at a rate of 2 bits, determines the publicly known bits 00 but uncertain of the information bits because needs to receive at 4 bits.

Figure 3.8: Decoding at Bob and Eve respectively for $(4, 2)$ wiretap code. Therefore the system is secure for a rate of 2 bits.

the instantaneous capacity at the eavesdropper and destination are $R_S(3, 1)$, or $R_S(5, 3)$ as a result of varying channel conditions. In the standard formulation, these distinct channel conditions are treated quite equally and the system is secure since the secrecy outage constraint $R_S \geq 2$ is satisfied.

In this Chapter we offer a tighter definition of secrecy outage and form a different secrecy outage formulation, where we consider not only choosing a target secrecy rate that represents the difference between the main channel and eavesdropper channel, but rather the choice of two individual target secrecy rates. Hence, rather than one degree of freedom, R_0, as in the outage formulation shown in, for example, [11], we introduce two degrees of freedom (R_{B0}, R_{E0}) for a system not to be an outage; in other words, Bob must be able to decode the message while Eve is unable to decode the message. This translates to the notion of a tighter secrecy region than [11], shown in the rectangular shaded region in Fig 3.9. For example if a $R_S(4, 2)$ wiretap code is employed, instantaneous channel conditions leading to the occurrence of $R_S(3, 1)$ or $R_S(5, 3)$ would be deemed an outage in our secrecy

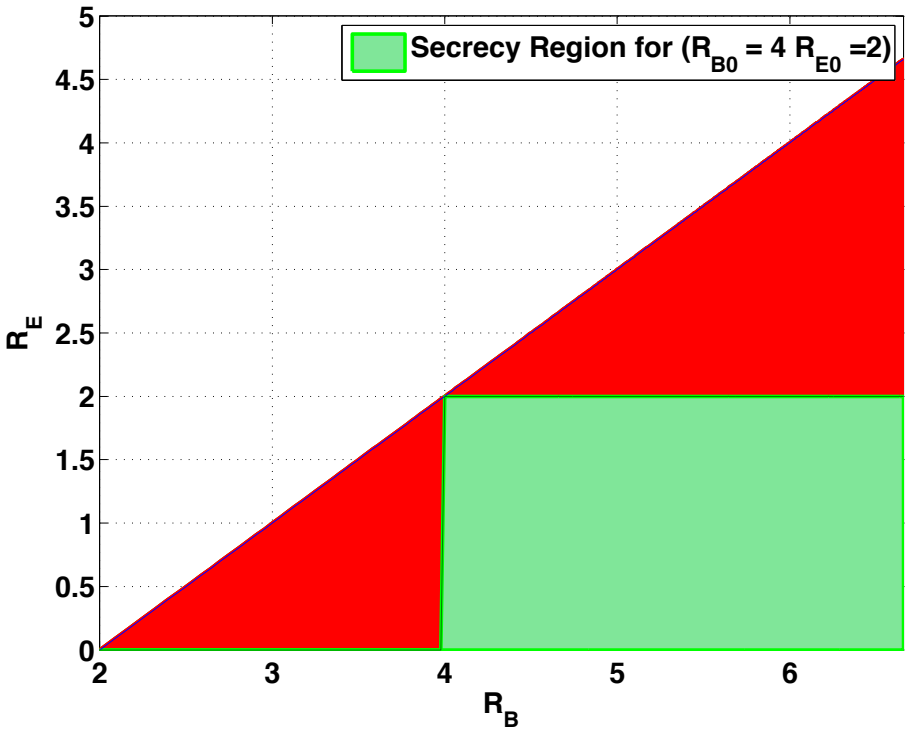


Figure 3.9: Secrecy region for $R_0 = 2$, where the lighter shaded rectangular (green) region shows the secrecy region for a system design for the wiretap code $(R_{B0} = 4, R_{E0} = 2)$. The darker shaded triangular (red) regions show the areas of outage not considered in the standard formulation, where the upper triangle represents the eavesdropper rate being too high ($R_E > 2$) as the cause of an outage and the lower triangle represents where the destination rate being too low ($R_B < 4$) is the cause of an outage.

rate pair formulation because, in the former case, $R_B < R_{B0}$, and in the latter case, $R_E > R_{E0}$.

The secrecy outage definition of [11] is sufficient if R_B or R_E is known (i.e. channel state information (CSI)), in which case the choice of R_0 fixes the other rate (R_{E0} or R_{B0}, respectively) and hence specifies the pair, in which case our definition is equivalent to the standard definition. However, if neither R_B nor R_E is known (i.e no channel state information at the transmitter [11, pg 199]), then we would argue that our stricter definition is required. This will be demonstrated concretely in the Secrecy Rate Pair Formulation (Section 3.4).

The two different outage regions $R_B < R_{B0}$ and $R_E > R_{E0}$ also come with a quite different costs, as interception of the message is more important than simply the dropping of the packet (in which retransmission can be employed). In particular, we can exploit the use of automatic repeat request (ARQ) schemes [14], keeping the eavesdropper intercept probability below the outage constraint while maximizing throughput to the destination which will be explained in Section 3.4. In Section 3.4 we will explore two widely used hybrid ARQ systems: basic hybrid ARQ, where there is no memory and the receiver only provides the source with a single bit of feedback telling whether the packet was received correctly, and hybrid ARQ with soft combining, where the receiver also buffers receptions and uses packet combining over multiple transmissions to increase the SNR of the received message.

3.3.1 System Model

In this section we discuss the system model used throughout this Chapter and then consider secrecy outage under the standard and proposed rate pair approaches. We consider a wireless network where a source node A (Alice) wishes to communicate to a destination node B (Bob) in the presence of a passive eavesdropper node E (Eve).

Each transmitted symbol of the source node A is denoted by $x_i^{(A)}$, and each received symbol for the destination node B and eavesdropper E will be denoted by $y_i^{(B)}$, and $y_i^{(E)}$ respectively. We assume frequency non-selective Rayleigh fading between the active transmitter and each of the receivers, where $h_{X,Y}$ is the normalized ($E[|h_{X,Y}|^2] = 1$) multipath fading on a link from a given transmitter X to a given receiver Y and is a complex zero-mean Gaussian random variable. The multipath fading is assumed to be constant over the duration of a codeword and independent for each distinct transmitter-receiver pair. The received signal at the

destination and eavesdropper are, respectively:

$$y_i^{(B)} = \frac{h_{A,B}}{\sqrt{d_{A,B}^{\alpha}}}\sqrt{E_s}x_i^{(A)} + n_i^{(B)}$$
$$y_i^{(E)} = \frac{h_{A,E}}{\sqrt{d_{A,E}^{\alpha}}}\sqrt{E_s}x_i^{(A)} + n_i^{(E)} \tag{3.3}$$

where $d_{X,Y}$ is the distance between nodes X and Y, α is the path-loss exponent, E_s is the transmitted energy per symbol, $\{n_i^{(B)}\}$ and $\{n_i^{(E)}\}$ are independent sequences of independent and identically distributed (i.i.d) zero-mean complex Gaussian random variables with variance N_0, and $|h_{X,Y}|^2$ is an exponentially distributed random variable with parameter 1. The locations of the system nodes are assumed to be known, including that of the eavesdropper. However the channel gains $h_{A,E}$ and $h_{A,B}$ are assumed to be unknown at the transmitter (i.e. no transmitter channel state information). When multiple packets are considered in the ARQ systems, it will be assumed that the fading affecting different packets is independent.

3.3.2 Standard Secrecy Rate Constraint

Since we consider a fading environment with additive white Gaussian noise, a Gaussian wiretap model is used, where the instantaneous secrecy rate conditioned on the fading is [42]:

$$R_S = \log_2(1 + \gamma_{AB}) - \log_2(1 + \gamma_{AE}) \tag{3.4}$$

where $\gamma_{AB} \triangleq \frac{|h_{A,B}|^2 E_s}{N_0 d_{A,B}^{\alpha}}$, and $\gamma_{AE} \triangleq \frac{|h_{A,E}|^2 E_s}{N_0 d_{A,E}^{\alpha}}$. As defined in [11, 12], the secrecy outage is defined as the probability that the fading values $h_{A,B}$, and $h_{A,E}$ are such that R_S is below a targeted secrecy rate R_0, which yields:

$$
\begin{aligned}
P_{out} &= P(R_S < R_0) \\
&= P(\log_2(1+\gamma_{AB}) - \log_2(1+\gamma_{AE}) < R_0) \\
&= P\left(\frac{1+\frac{|h_{A,B}|^2 E_s}{N_0 d_{A,B}^{\alpha}}}{1+\frac{|h_{A,E}|^2 E_s}{N_0 d_{A,E}^{\alpha}}} < 2^{R_0}\right) = 1 - \frac{e^{\frac{-2^{R_0} N_0 d_{A,B}^{\alpha} + N_0 d_{A,B}^{\alpha}}{E_s}}}{1+\frac{2^{R_0} d_{A,B}^{\alpha}}{d_{A,E}^{\alpha}}}
\end{aligned} \tag{3.5}
$$

For example, consider the case where the target secrecy rate is $R_0 = 2$. Secrecy is achieved when $R_S \geq 2$, and outage occurs if $R_S < 2$. In Fig. 3.9, the secrecy event for $R_0 = 2$ is shown. The unshaded region represents the area where the system is in outage ($R_S < R_0$), and the total shaded region represents where the system is secure ($R_S \geq R_0$).

3.3.3 Secrecy Rate Pair Constraint

Motivated by the inability to guarantee secrecy for all $R_S > R_0$ when transmitter CSI is unavailable, as described in Section 3.1, we thus consider a tighter definition for secrecy outage. In our formulation we consider secrecy in terms of a pair of two individual rates (R_{B0}, R_{E0}), whose secrecy region is shown in the light shaded rectangular region of Fig. 3.9. In particular, we will seek to constrain the information leakage to an eavesdropper ($R_E \leq R_{E0}$) while transmitting a certain amount of information to the destination ($R_B \geq R_{B0}$). The outage probability of this system is then defined as the probability of two independent events:

$$
\begin{aligned}
P_{out} &= 1 - P(\{\log_2(1+\gamma_{AB}) \geq R_{B0}\} \bigcap \{\log_2(1+\gamma_{AE}) < R_{E0}\}) \\
&= 1 - \left(e^{\frac{-(2^{R_{B0}}-1) N_0 d_{A,B}^{\alpha}}{E_s}}\right)\left(1 - e^{\frac{-(2^{R_{E0}}-1) N_0 d_{A,E}^{\alpha}}{E_s}}\right)
\end{aligned} \tag{3.6}
$$

When there is no channel state information available at the transmitter, our secrecy rate pair construction is important for a reliable and secure system. We first consider a system with Alice and Bob a unit distance apart, Alice and Eve fixed at four

units apart, a pathloss exponent of $\alpha = 2$, a transmit SNR of 10 dB, and an outage secrecy constraint of $\epsilon = 0.01$. In a wiretap code design, we must design a rate pair (R_{B0}, R_{E0}) that meets the secrecy outage constraint. But for the standard metric, we are free to choose from a wide range of pairs to meet that constraint, as follows. First, one sets $P(R_S < R_0) = 0.01$ in (3.5), and solves for R_0. For the example here, this yields $R_0 = 0.08$. But this does not uniquely determine the pair (R_{B0}, R_{E0}), as any pair such that $R_{B0} - R_{E0} = 0.08$ satisfies $R_S = 0.08$. In Fig. 3.10, we consider the secrecy outage performance for different possible pairs such that $R_S = 0.08$; in particular, the independent variable (x-axis) is R_{B0}, which then determines R_{E0} as $R_{B0} - 0.08$. For small R_{B0}, the system does not require a very high rate at Bob, resulting in a low probability of outage at Bob, but, in turn, this makes it easy for Eve to intercept the packet. For a large R_{B0}, one can then employ a large R_{E0}, thereby thwarting Eve's attempts to intercept the packet, but now Bob's probability of outage is unacceptably high. Note that there is no R_{B0} for which the secrecy outage constraint is met due to the different (and, we would claim, insufficient) secrecy outage region employed for the selection of R_0 in this application (no CSI at the transmitter), as shown in Fig. 3.9.

3.4 Secrecy with ARQ

The two different outage regions $R_B < R_{B0}$ and $R_E > R_{E0}$ also come with a quite different costs, as interception of the message is more important than simply the dropping of the packet (in which retransmission can be employed). In particular, we can exploit the use of automatic repeat request (ARQ) schemes [14], keeping the eavesdropper intercept probability below the outage constraint while maximizing throughput to the destination. In [43], results were shown to support that hybrid ARQ systems for the Gaussian collision channel are not interference-limited compared to conventional code division multiple access (CDMA). In addi-

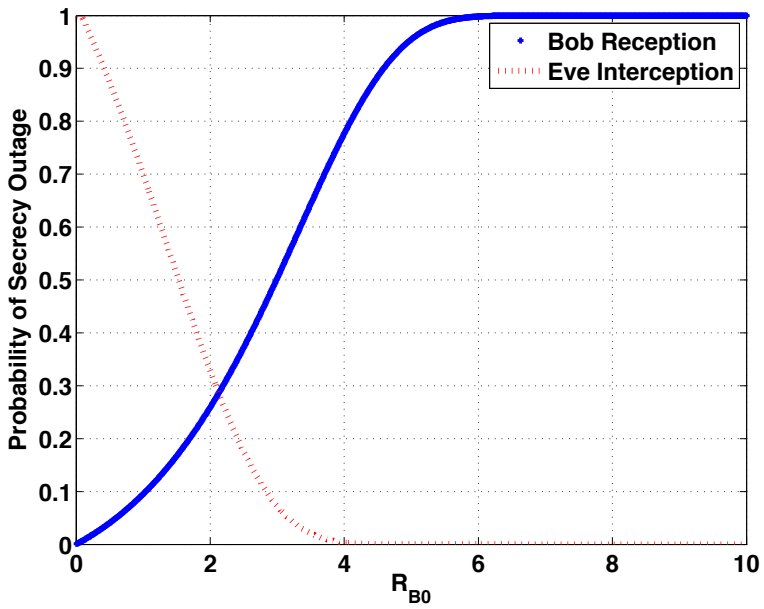


Figure 3.10: Probability of secrecy outage as a function of the rate R_{B0}. The R_0 from (3.5) that meets the outage constraint $\epsilon = 0.01$ is $R_0 = 0.08$; thus, for each R_{B0}, $R_{E0} = R_{B0} - 0.08$. The probability of outage at Bob and the complimentary intercept probability at Eve is then shown for various possible wiretap codes (R_{E0}, R_{B0}). None of the prescribed wiretap rate codes are sufficient in guaranteeing the desired secrecy because of the different definition of the outage region in Fig. 3.9; either Eve's probability of intercept is well above 0.01 or Bob's probability of outage is intolerable.

tion, Hybrid ARQ systems were considered for Rayleigh Block Fading channels in [44], where the advantage of throughput for such a system, especially at practical signal-to-noise ratio (SNR) of interest is shown. Also, [45] considered hybrid ARQ protocols on Gaussian block-fading channels to establish connection and secrecy outage, which characterizes the reliability and confidentially, respectively, of the legitimate receiver in the presence of an eavesdropper.

Differently than [45, 46] in our work we consider the aforementioned secrecy rate pair constraint formulation as a function of an eavesdropper at a varying distance away from the source. Given an eavesdropper location, it is of great interest to determine the maximal secure throughput while meeting the intercept prob-

ability constraint. Although, as stated earlier, many secrecy rate pairs can yield the same instantaneous secrecy capacity, not all are created equal as the amount of "goodput" or amount of information reliably transmitted to Bob influences the optimal secrecy rate pair and overall maximum secure throughput. Additionally, important especially to information-theoretic security is the case of a more complex eavesdropper; therefore, we will consider the case in which the eavesdropper uses a more robust receiver in comparison to the intended receiver.

In the following sections we will explore two widely used hybrid ARQ systems: basic hybrid ARQ (Section 3.4.1), where there is no memory and the receiver only provides the source with a single bit of feedback telling whether the packet was received correctly, and hybrid ARQ with soft combining (Section 3.4.2), where the receiver also buffers receptions and uses packet combining over multiple transmissions to increase the SNR of the received message. Differently, we will focus on applying these HARQ techniques given the secrecy rate pair constraint aforementioned as will be demonstrated concretely later in this Chapter.

3.4.1 Basic Hybrid ARQ

An investigation into Fig. 3.9 shows that the unsecured dark shaded region (red) has two sub regions that represent two events with very different implications in the application. The upper dark shaded triangle represents the region where the eavesdropper rate (R_E) is above the threshold (R_{E0}). As discussed earlier, this is the most costly form of outage: a secrecy breach. The lower dark shaded triangle in Fig. 3.9 represents the area where the destination rate (R_B) is below a targeted threshold (R_{B0}). In this region, automatic repeat request (ARQ) along with retransmissions can be employed by the transmitter to achieve secrecy. If the instantaneous SNR at the destination is below the threshold, an ARQ is triggered to the transmitter to initiate a retransmission to the destination. In a basic

Hybrid ARQ (HARQ) scheme, the destination notifies the receiver if it receives the packet successfully through the use of a positive acknowledgement/negative acknowledgment (ACK/NAK) bit. We assume the feedback channel is noiseless; therefore, the feedback is perfectly reliable. If the source receives a NAK, then the source retransmits the same message until the destination successfully receives the message, designated by an ACK. This leads to an extension of our secrecy rate pair formulation: we put a constraint on the eavesdropper's ability to intercept a packet, including both the initial phase and retransmissions, while maximizing the system throughput. The probability that the eavesdropper rate is above the targeted threshold for a given transmission is:

$$P\left(\log_2(1+\gamma_{AE}) \geq R_{E0}\right) = P\left(1 + \frac{|h_{A,E}|^2 E_s}{N_0 d_{A,E}^{\alpha}} \geq 2^{R_{E0}}\right) = e^{\frac{-\left(2^{R_{E0}}-1\right) N_0 d_{A,E}^{\alpha}}{E_s}} \tag{3.7}$$

Likewise the probability of success at the destination for a given transmission is:

$$P\big(\log_2(1+\gamma_{AB}) \geq R_{B0}\big) = e^{\frac{-\left(2^{R_{B0}}-1\right) N_0 d_{A,B}^{\alpha}}{E_s}} \tag{3.8}$$

For simplicity of notation we will use $\tau_E = \frac{(2^{R_{E0}}-1) N_0 d_{A,E}^{\alpha}}{E_s}$ and $\tau_B = \frac{(2^{R_{B0}}-1) N_0 d_{A,B}^{\alpha}}{E_s}$, the thresholds on the fading for the Alice to Bob and Alice to Eve channels for packet reception or packet interception, respectively, use throughout the Chapter. For simplicity, define the following events:

- E_i: the packet is decoded by Eve on the i^{th} transmission
- B_i: the packet is decoded by Bob on the i^{th} transmission
- I_i: the packet is intercepted by Eve for the *first* time on the i^{th} transmission.

Noting that $I_1, I_2, \cdots$ are mutually exclusive and recalling the assumption that the fading is independent for different transmissions of the packet:

$$\begin{aligned}
P(I) &= P\Big(\bigcup_{i=1}^{\infty} I_i\Big) = \sum_{i=1}^{\infty} P(I_i) \\
&= \sum_{i=1}^{\infty} P(\log_2(1+\gamma_{AB}) < R_{B0})^{i-1} P(\log_2(1+\gamma_{AE}) \geq R_{E0}) \\
&\qquad P(\log_2(1+\gamma_{AE}) < R_{E0})^{i-1} \\
&= P(\log_2(1+\gamma_{AE}) \geq R_{E0}) \sum_{i=0}^{\infty} P(\log_2(1+\gamma_{AB}) < R_{B0})^{i} \\
&\qquad\qquad P(\log_2(1+\gamma_{AE}) < R_{E0})^{i} \\
&= \frac{P(R_E \geq R_{E0})}{1-\big(1-P(R_B \geq R_{B0})\big)\big(1-P(R_E \geq R_{E0})\big)} \\
&= \frac{e^{-\tau_E}}{1-\big(1-e^{-\tau_B}\big)\big(1-e^{-\tau_E}\big)} < \epsilon
\end{aligned} \tag{3.9}$$

Our goal is to pick the pair (R_{B0}, R_{E0}) such that $P(I) < \epsilon$, while maximizing the average reliable throughput, which is simply the probability of successful reception times the rate: $e^{-\tau_B} R_0 = e^{-\tau_B}(R_{B0} - R_{E0})$.

As discussed throughout the Chapter, we can exploit the use of HARQ to improve the secrecy performance of the system. For the evaluation of this approach, we consider the following environment: source and destination nodes at a unit distance, the eavesdropper at some variable distance away from the source, a path loss exponent of $\alpha = 2$ and $\frac{E_S}{N_0} = 10$ dB. Fig. 3.11 shows the probability of packet intercept achieved as a function of distance from Alice to Eve, where the intercept probability constraint is set to $\epsilon = 0.01$. Recall that this intercept constraint must be met for a given packet not just for each individual transmission, but also for the combination of the original and all retransmissions; in other words, Eve has intercepted a packet if she obtains it on any transmission. This indicates why this intercept probability is a function of both R_{E0} *and* R_{B0}, as R_{B0} determines the probability that Alice has to re-transmit a packet and hence impacts the number

of chances Eve gets to intercept it. Among those rate pairs (R_{B0}, R_{E0}) meeting the intercept constraint, the one providing the maximum throughput is selected.

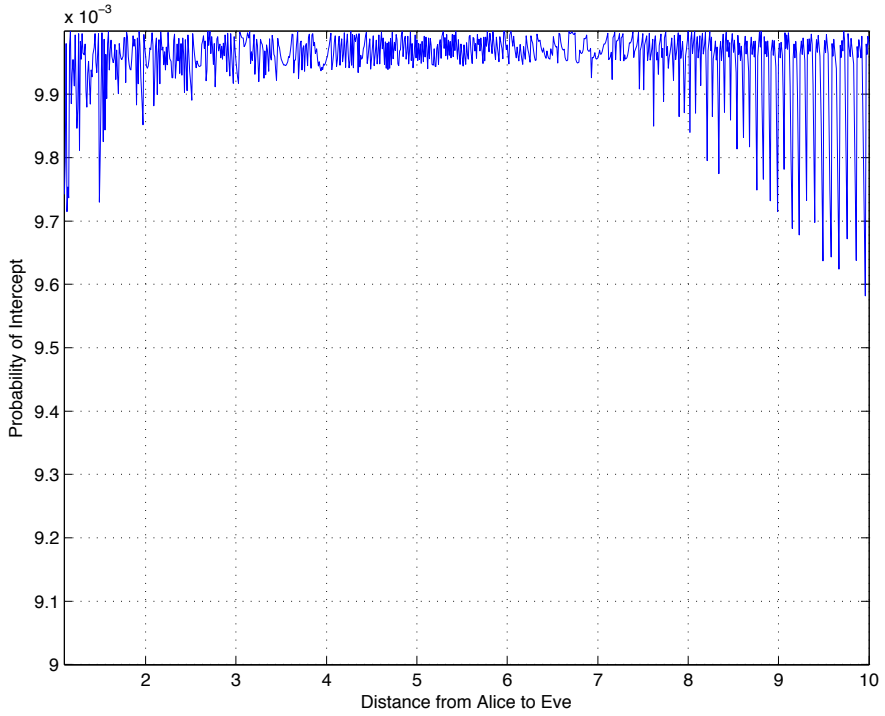


Figure 3.11: Probability of intercept of the message by the eavesdropper in the basic HARQ system for the optimum secrecy rate pair (R_B, R_E) as a function of the distance of the eavesdropper from the source 0.01 to 10 in 0.01 steps. To the find the optimal pair, rates R_B and R_E were varied from 0.01 to 10.00 with 1000 points considered for each individual rate to form a 1000 by 1000 rate pair grid. The rate pair selected provides the maximum throughput while guaranteeing the intercept probability $\epsilon = 0.01$ at Eve. As expected, the intercept probability constraint is always met.

Fig. 3.12 illustrates the maximum throughout for different distances of the eavesdropper away from the source while satisfying an intercept probability of $\epsilon = 0.01$ for various transmit SNR. The plot shows that, as the SNR increases the maximum throughput we can achieve greatly improves, especially as Eve gets farther away from Alice. However, also as expected in a security setting, there are diminishing returns as the SNR becomes very large, as the increased transmit

power helps both the receiver and the eavesdropper. Notably, the secrecy rates obtained for the same distance structure as those used in Fig. 3.10 are significantly higher than the traditional scheme ($R_0 = 0.08$). This is largely due to the ability to perform retransmissions, the power of which has been observed in previous security work for secure throughput [46] and key establishment [47]. In Fig. 3.13, we assume a fixed transmit power $\frac{E_S}{N_0} = 10$ dB, but consider various path loss exponents to show the effect on system performance as the transmit signals propagates through different environments. As expected, as the path loss exponent increases, the difference in effective average SNR between the main channel and eavesdropper channel increases (since Eve is generally further away from Alice than Bob), and thus the reliable secure throughput increases.

3.4.2 Hybrid ARQ: Soft Combining

Rather than discarding a packet, a receiver can store previous transmissions as shown in Fig. 3.14. Once received samples are stored, the receiver can apply soft combining to decode the message from the source. Various transmission techniques exist to support soft combining at the receiver. Often, every transmission sent by the source has the same information to increase the overall SNR of the received message. Another commonly used technique is incremental redundancy (IR) [43], where the initial transmission has the minimum redundant data, and every retransmission onward incrementally adds more redundancy to increase the likelihood of decoding the information correctly. In our work we consider the former case, where the information is repeated, although the incremental redundancy case follows similarly, but with more complicated final expressions requiring numerical integration.

We analyze system performance when soft combining is implemented for the destination or eavesdropper. Of particular interest is how soft combining at the

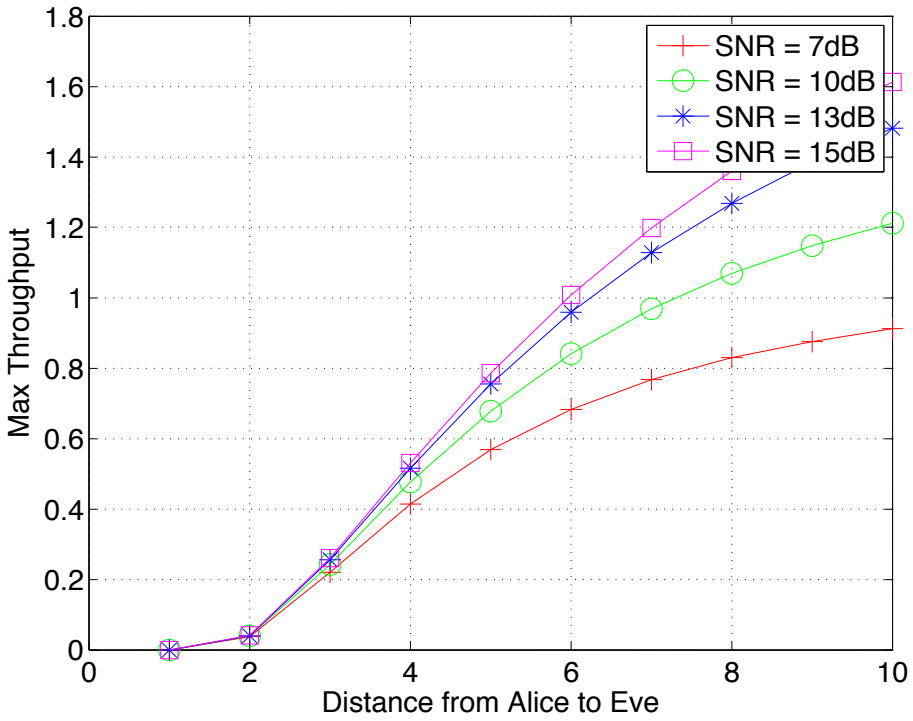


Figure 3.12: Maximum secure throughput with basic HARQ (i.e. neither Bob nor Eve employ soft combining) as a function of the distance from Alice to Eve for various $\frac{E_s}{N_0}$. The probability of intercept constraint for the eavesdropper is set to $\epsilon = 0.01$, the path loss exponent is $\alpha = 2$, and the distance from Alice to Bob is one. In each case, 1000 data points were considered. Note the significant rate gain provided by this approach over the traditional design when the distance from Alice to Eve is 4.0 (yielding the same distance structure as considered for the generation of Fig. 3.10).

eavesdropper, which improves its intercept capabilities, can limit the secrecy rate. Thus, we first consider the case where only the eavesdropper employs soft packet combining. Consider the event I_2, the probability of first intercept on the first retransmission:

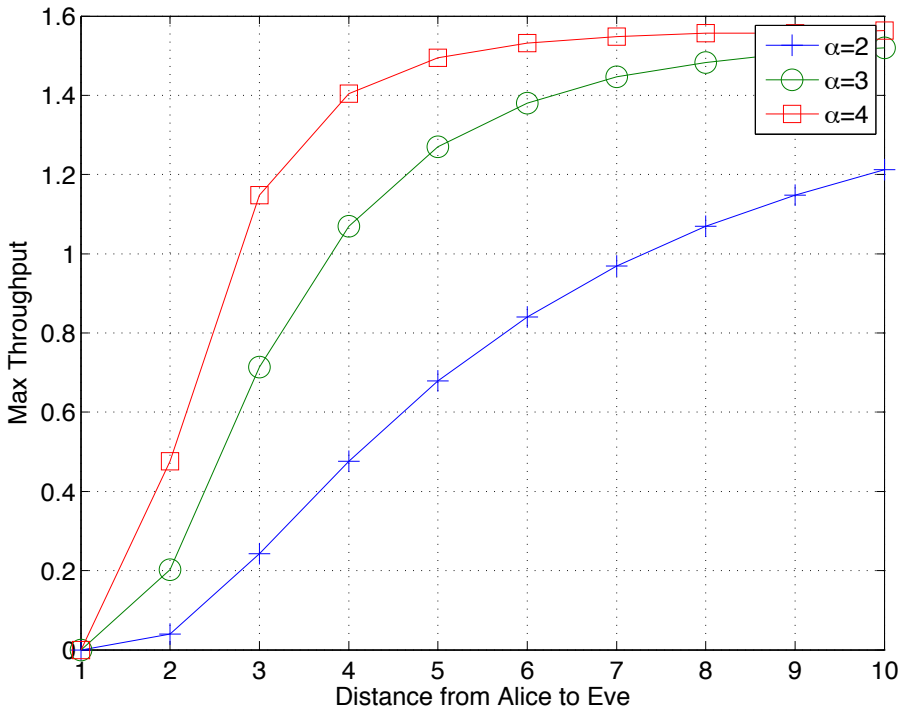


Figure 3.13: Maximum secure throughput with basic HARQ (i.e. neither Bob nor Eve employ soft combining) as a function of the distance from Alice to Eve for various α. The probability of intercept constraint for the eavesdropper is set to $\epsilon = 0.01$, the SNR is $\frac{E_s}{N_0} = 10$ dB, and the distance from Alice to Bob is one. In each case, 1000 data points were considered. When α gets larger, the maximum reliable secure throughput increases, as the SNR difference between the main and eavesdropper channel grows.

$$\begin{aligned} P(I_2) &= P(E_2 \bigcap \overline{E_1} \bigcap \overline{B_1}) = P(\overline{B_1}) P(E_2 \bigcap \overline{E_1}) \\ &= P(\overline{B_1}) P(\{\log_2(1+\gamma_{AE}^{(1)}+\gamma_{AE}^{(2)}) \geq R_{E0}\} \bigcap \{\log_2(1+\gamma_{AE}^{(1)}) < R_{E0}\}) \\ &= P(\overline{B_1}) \int_0^{\tau_E} \int_{\tau_E - x}^{\infty} e^{-x} e^{-y} dy dx \\ &= \left(1 - e^{-\tau_B}\right) \tau_E e^{-\tau_E} \end{aligned} \tag{3.10}$$

where, recall that τ_B and τ_E are the fading gain thresholds, as defined in Section 3.4.1. Extending from the binary case, we consider the event I_N, which is the event that the eavesdropper intercepts the packet for the first time on the N^{th} transmis-

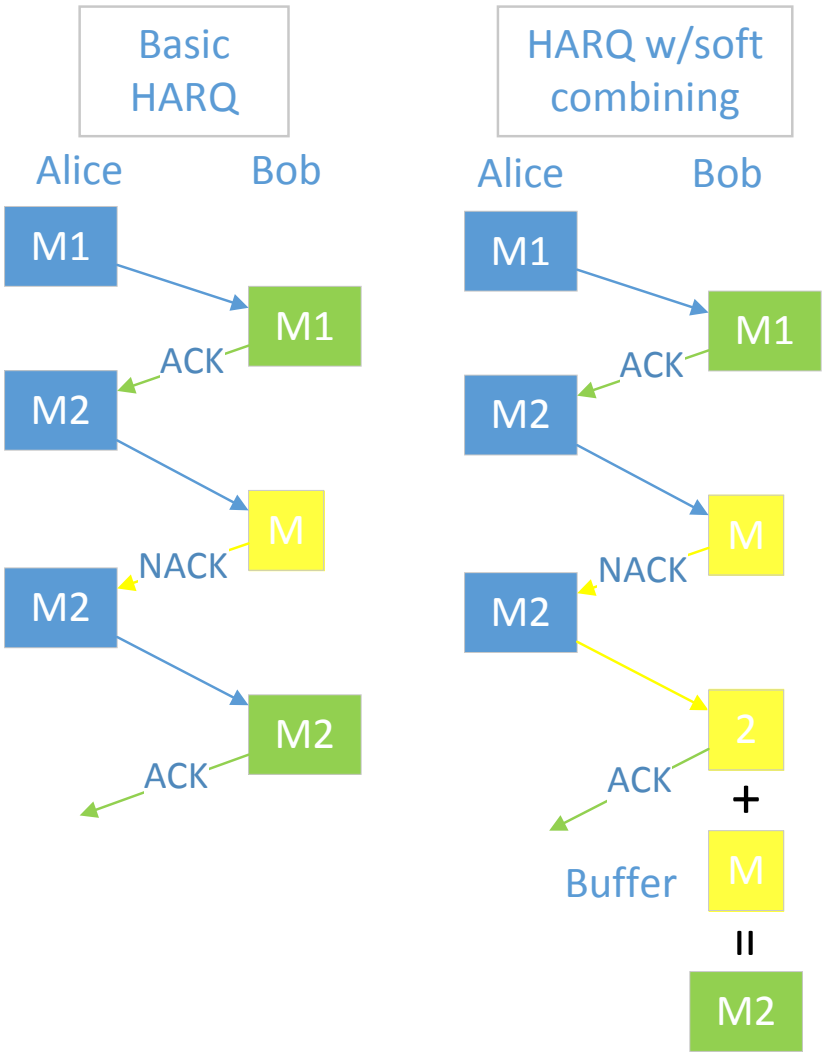


Figure 3.14: Basic HARQ and HARQ with soft combining are shown. In both schemes, Bob sends Alice an ACK if the message is receive successfully and a NACK if unsuccessful. In the case of Basic HARQ, Bob discards messages if they are receive unsuccessful but in HARQ with soft combining, Bob buffers incomplete receptions and uses packet combining over multiple transmissions to increase the SNR of the received message.

sion:

$$P(I_N) = P(E_N \cap \overline{E}_{N-1} \cap ... \overline{E}_1) P(\overline{B}_{N-1} \cap \overline{B}_{N-2} \cap ... \overline{B_1}) \tag{3.11}$$

Recall that each fading variable squared $|h_{X,Y}|^2$ is exponentially distributed with parameter 1. The summation of N independent exponential random variables is a Chi Square Distribution with $2N$ degrees of freedom, where $Z = \sum_{n=1}^{N} X_n^2$, with $X_n \backsim N(0, \sigma^2)$, $\sigma = \frac{1}{2}$ [48, pg 41]. With $f_Z(x)$ the probability density function of Z, evaluating the first term in (3.11) yields:

$$\begin{aligned}
P(E_N \bigcap \overline{E}_{N-1} \bigcap ... \overline{E}_1) &= P\left(\left\{ \log_2 \left(1 + \sum_{i=1}^{N} |h_{A,E}^{(i)}|^2 \right) \geq \tau_E \right\} \right) \\
&\qquad \bigcap \left\{ \log_2 \left(1 + \sum_{i=1}^{N-1} |h_{A,E}^{(i)}|^2 \right) < \tau_E \right\} \\
&= \int_0^{\tau_E} \int_{\tau_E - x}^{\infty} f_Z(x) e^{-y} dy\, dx = \int_0^{\tau_E} f_Z(x) e^{-(\tau_E - x)} dx \\
&= \frac{e^{-\tau_E}}{\sigma^{2N} 2^N \Gamma(N)} \int_0^{\tau_E} x^{N-1} e^{-x\left(\frac{1}{2\sigma^2} - 1\right)} dx \\
&= \frac{e^{-\tau_E}}{\sigma^{2N} 2^N \Gamma(N)} \left[\frac{(N-1)!}{a^N} - e^{-\tau_E a} \left(\sum_{k=0}^{N-1} \frac{\tau_E^{N-k-1} (N-1)!}{a^{k+1} (N-1-k)!} \right) \right]
\end{aligned} \tag{3.12}$$

where $\Gamma(N) = (N-1)!$, and $a = \frac{1}{2\sigma^2} - 1$. If Bob still employs basic ARQ (i.e. no soft combining), the second term in (3.11) is:

$$P(\overline{B}_{N-1} \bigcap \overline{B}_{N-2} \bigcap ... \overline{B_1}) = \left(1 - e^{-\tau_B}\right)^{N-1} \tag{3.13}$$

Since the event of *first* intercept on the i^{th} transmission is mutually exclusive of the *first* intercept on any other transmission, the final expression for the probability of intercept for the case where the destination does not store packets and the eavesdropper stores packets and employs soft packet combining is:

$$\begin{aligned}
\sum_{N=1}^{\infty} P(I_N) = \sum_{N=1}^{\infty} &\left(1 - e^{-\tau_B}\right)^{N-1} \frac{e^{-\tau_E}}{\sigma^{2N} 2^N \Gamma(N)} \\
&\left[\frac{(N-1)!}{a^N} - e^{-\tau_E a} \left(\sum_{k=0}^{N-1} \frac{\tau_E^{N-k-1} (N-1)!}{a^{k+1} (N-1-k)!} \right) \right]
\end{aligned} \tag{3.14}$$

Finally, we consider the case where the destination additionally has the ability to do packet combining; then,

$$P(\overline{B}_{N-1}\bigcap\overline{B}_{N-2}\bigcap...\overline{B}_1) = \frac{1}{\sigma^{2N}2^N\Gamma(N)} \left[\frac{(N-1)!}{b^N} - e^{-\tau_B b}\left(\sum_{k=0}^{n-1}\frac{\tau_B^{N-k-1}(N-1)!}{b^{k+1}(N-1-k)!}\right)\right] \quad (3.15)$$

where $b = \frac{1}{2\sigma^2}$, from which the analog to (3.14) is derived.

Lastly, Fig. 3.15 shows the maximum throughput when HARQ with soft combining is use by one or both receivers over varying distances of Eve from Alice while satisfying the intercept probability constraint. Fig. 3.15 illustrates the decrease in throughput when Eve has the ability to buffer packets and employ soft combining; however, the throughput is still significantly higher than that obtained by a one-shot scheme designed with the traditional approach.

3.5 Secrecy with ARQ for a Two-Hop Network

Especially in mesh or adhoc networks, limited direct communication can exist between the source and the destination, perhaps due to bad geometries, distance and/or fading. In the case of limited communication, the main link is at an outage state or more critical, high secrecy threat; the eavesdropper might have a high probability of intercept on the main link. In these situations a relay node can assist in the communication of the message. These multi-hop transmissions (e.g. two-hop transmissions) fit into a broader class of transmission protocols called cooperative communications [49]. In [50, 51], cooperative diversity was shown to increase capacity and robustness for mobile users, where cooperation helps reduce the total power for users to achieve a certain rate pair than with no cooperation, thus extending battery life of mobile devices.

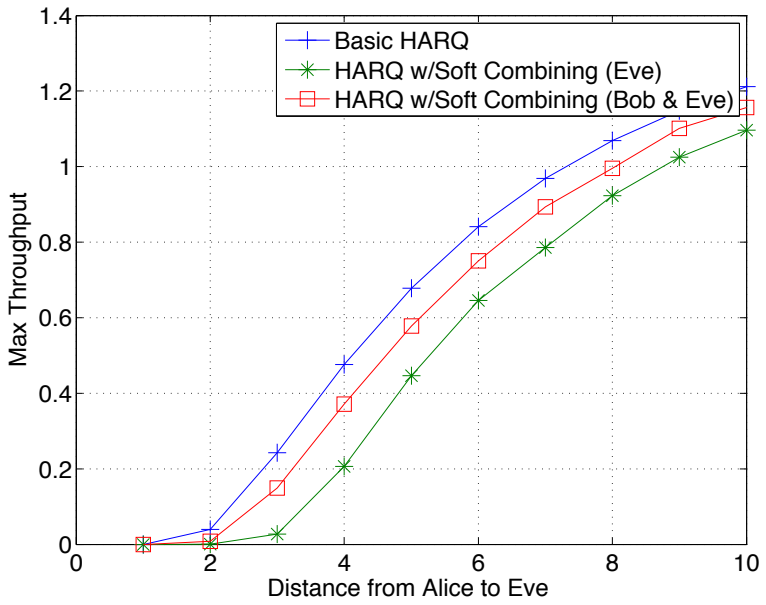


Figure 3.15: Maximum secure throughput with HARQ with soft combining at Eve, as a function of the distance from Alice to Eve. The probability of intercept constraint for the eavesdropper is set to $\epsilon = 0.01$, the SNR is $\frac{E_s}{N_0} = 10$ dB, $\alpha = 2.0$ and the distance from Alice to Bob is one. In each case, 1000 data points were considered.

In [52], three different methods were considered, cooperative jamming (CJ), amplitude-and-forward (AF) and decode-and-forward (DF). AF is a strategy used where relay nodes amplify the noisy received signal and forward the noisy signal to the destination. Differently, in decode and forward, the relay node decodes the received signal and, if correctly decoded, forwards the noiseless signal to the destination. In [52], the authors compared the maximum secrecy rate from the aforementioned cooperative techniques as opposed to direct transmission to the destination, assuming optimal power allocation to the transmitting nodes. Also discussed was the minimal power allocation to transmitting nodes to meet a specific secrecy rate, but the authors assumed that channel state information for the eavesdropper is known. In this dissertation, we consider unknown channel state information about the eavesdropper. In [53], a secure communication game where

the relay helps the eavesdropper was investigated and showed the achievable secrecy rate. Then [54] considered multiple access channels where multiple users communicate with a common receiver in the presence of an eavesdropper, and the optimal transmit power allocation policy is chosen to maximize the secrecy sum-rate.

Differently here we extend the existing secrecy rate pair hybrid ARQ work presented earlier to the two-hop network. Consider the two-hop network where the source communicates via a relay because of either a bad fade, security threat, or bad distance geometry to the destination. In the first hop, the source communicates to the relay and the second hop, the relay communicates to the destination, where the two-hop communication will be commonly referred to as the end-to-end path. During the two-hop communication, potentially two eavesdroppers independently listen to each successive transmission. As in previous work, high importance is placed on security: the eavesdropper at an outage. Security is a great challenge in the described scenario because of the increase in the number of nodes that the message traverses through in the end-to-end path. In addition, given a total eavesdropper outage constraint on the end-to-end path, allocating the outage constraint across each link is no trivial task. Moreover while maintaining outage on each link at the eavesdropper, optimization of the end-to-end throughput requires great attention because these pairs corresponds to the secrecy rate pairs for the intended receivers and eavesdroppers. In summary the problem is formulated as the following: maximize the overall secrecy throughput of the end-to-end path while constraining the total end-to-end intercept probability:

$$\min \max \left\{ e^{\tau_{B_1}} \left(R_{B_1} - R_{E_1} \right), e^{\tau_{B_2}} \left(R_{B_2} - R_{E_2} \right) \right\} \tag{3.16}$$

$$\text{s.t.} \quad \epsilon_T = \epsilon_1 + \epsilon_2 \tag{3.17}$$

where R_{B_i} and R_{E_i} represent the capacity of the legitimate transmitter receiver pair and the capacity of the transmitter eavesdropper pair on link i respectively, ϵ_T represents the total end-to-end intercept outage constraint partition to the relay on link 1 and the destination on link 2, ϵ_1 and ϵ_2 respectively. Alternatively the constraint (3.17) can be expanded to:

$$\epsilon_T = \frac{e^{-\tau_{E_1}}}{1-(1-e^{-\tau_{B_1}})(1-e^{-\tau_{E_1}})} + \frac{e^{-\tau_{E_2}}}{1-(1-e^{-\tau_{B_2}})(1-e^{-\tau_{E_2}})} \tag{3.18}$$

For simplicity of notation we will use $\tau_{E_i} = \frac{(2^{R_{E_i}}-1)N_0 d^{\alpha}_{A,E_i}}{E_S}$, $\tau_{B_i} = \frac{(2^{R_{B_i}}-1)N_0 d^{\alpha}_{A,B_i}}{E_S}$, the thresholds on the fading for the transmitter to the intended receiver i and transmitter to eavesdropper i channels for packet reception or packet interception, respectively. This sets the stage for an optimization problem where in the objective function we desire to figure out the best $(R^*_{B_1}, R^*_{E_1})$,$(R^*_{B_2}, R^*_{E_2})$ and ϵ_1, ϵ_2 for each link to satisfy the total ϵ_T constraint given. The first approach to solve this problem is a Lagrange multiplier solution (Appendix B) to figure out the optimal unknowns but a solution cannot be found analytically satisfying the necessary conditions:

$$\begin{aligned}
\lambda &\Longrightarrow \frac{e^{-\tau_{E_j}}}{e^{-\tau_{E_j}} + e^{-\tau_{B_j}} - e^{-\tau_{E_j}} e^{-\tau_{B_j}}} - \epsilon_T = 0 \\
\tau_{B_j} &\Longrightarrow -\left(e^{-\tau_{B_j}} \left[\log_2 \left(\frac{P_s \tau_{B_j} + N_0 d^{\alpha}_{A,B_j}}{N_0 d^{\alpha}_{A,B_j}} \right) - \log_2 \left(\frac{P_s \tau_{E_j} + N_0 d^{\alpha}_{A,E_j}}{N_0 d^{\alpha}_{A,E_j}} \right) \right] \right. \\
&\quad \left. + (1 - e^{-\tau_{B_j}}) \frac{P_s}{P_s \tau_{B_j} + N_0 d^{\alpha}_{A,B_j}} \right) - \lambda \frac{-e^{-\tau_{E_j}} (e^{-\tau_{E_j}} e^{-\tau_{B_j}} - e^{-\tau_{B_j}})}{(e^{-\tau_{B_j}} + e^{-\tau_{E_j}} - e^{-\tau_{E_j}} e^{-\tau_{B_j}})^2} = 0 \\
\tau_{E_j} &\Longrightarrow (1 - e^{-\tau_{B_j}}) \frac{P_s}{P_s \tau_{E_j} + N_0 d^{\alpha}_{A,E_j}} - \lambda \left(\frac{-e^{-\tau_{E_j}} (-e^{-\tau_{E_j}} + e^{-\tau_{E_j}} e^{-\tau_{B_j}})}{(e^{-\tau_{B_j}} + e^{-\tau_{E_j}} - e^{-\tau_{E_j}} e^{-\tau_{B_j}})^2} \right. \\
&\quad \left. - \frac{e^{-\tau_{E_j}}}{(e^{-\tau_{E_j}} + e^{-\tau_{B_j}} - e^{-\tau_{E_j}} e^{-\tau_{B_j}})} \right) = 0
\end{aligned} \tag{3.19}$$

The above problem requires the selection of five parameters (τ_{B_1}, τ_{E_1}, τ_{B_1}, τ_{E_2}, ϵ_1). These unknown variables are very difficult to solve analytically as well as numerically. These variables are highly dependent on the distances between the transmitter, receiver, and eavesdropper nodes, which have a large impact on the optimal τ_{B_i} and τ_{E_i}. Results from the one-hop problem show that for a fixed destination and intercept constraint, as the eavesdropper moves further away from the transmitter, the secrecy capacity increases because we can tolerate a lower fading constraint on the eavesdropper τ_E, thus reducing the rate R_E.

First, we revisit the original one-hop secrecy rate pair formulation but look for a solution where we can uniquely analytically figure out the optimal τ_B and τ_E that yields the optimal (T_P). Recall the following problem:

$$\max \quad e^{-\tau_B}\left(\log_2\left(1+\frac{\tau_B E_s}{N_0 d_{A,B}}\right)-\log_2\left(1+\frac{\tau_E E_s}{N_0 d_{A,E}}\right)\right) \tag{3.20}$$

$$\text{s.t.} \quad \frac{e^{-\tau_E}}{1-(1-e^{-\tau_B})(1-e^{-\tau_E})}=\epsilon_T \tag{3.21}$$

Since the intercept probability must be met on each and every hop, the eavesdropper intercept probability constraint from (3.21) can be used to derive τ_B as a function of τ_E and the intercept probability constraint (ϵ_T) as follows:

$$\begin{aligned}\tau_E &= \tau_B-\log_2(\epsilon_T)+\log_2(1+\epsilon_T e^{-\tau_B}-\epsilon_T)\\ &\approx \tau_B-\log_2(\epsilon_T)\end{aligned} \tag{3.22}$$

where (3.22) results from the fact that $\log_2(1+\epsilon_T e^{-\tau_B}-\epsilon_T)\approx\log_2(1)=0$. This approximation is validated in Fig. 3.16, where for small values of τ_B ($\tau_B<1$) the error is less than 0.009, and for larger values τ_B the error is less than 0.0145. Substituting τ_E into the objection function yields:

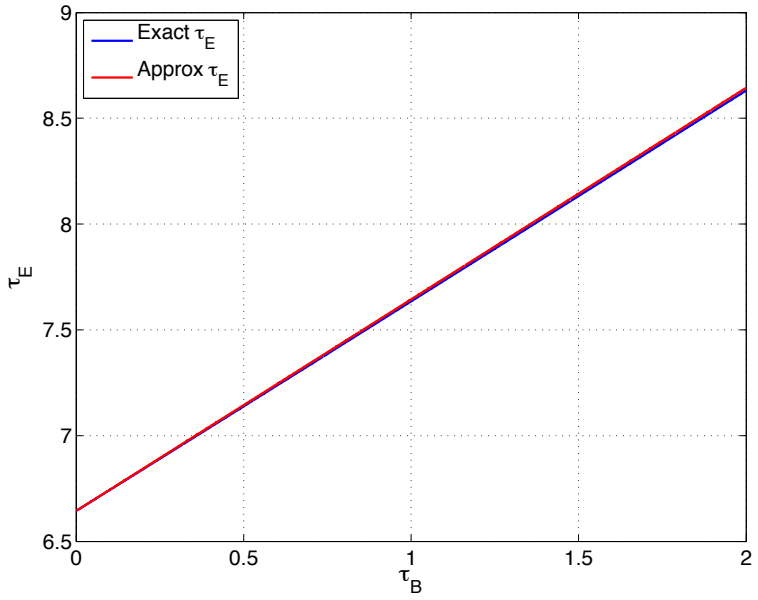


Figure 3.16: The fading constraint for Bob (τ_B) is plotted versus the fading constraint for Eve (τ_E), where the the approximation (3.22) for the intercept constraint is shown as a a very good estimate for the exact intercept constraint. This approximation is validated since small values of τ_B ($\tau_B < 1$) the error is less than 0.009, and for larger values τ_B the error is less than 0.0145.

$$\max \quad e^{-\tau_B}\left(\log_2\left(1+\frac{\tau_B E_s}{N_0 d_{A,B}}\right)-\log_2\left(1+\frac{(\tau_B-\log_2(\epsilon_T))E_s}{N_0 d_{A,E}}\right)\right) \tag{3.23}$$

where for positive throughput requires $\frac{\tau_B}{d_{A,B}} > \frac{\tau_B-\log_2(\epsilon_T)}{d_{A,E}}$. The trade-off for varying τ_B:

- *large* τ_B translates to a high rate from Alice to Bob; higher threshold on the fading, therefore higher probability of retransmissions; reliability concern ($e^{-\tau_B} \to 0$).

- *small* τ_B translates to a smaller rate from Alice to Bob; lower threshold on the fading, therefore higher probability of success of the first transmission.

Given the optimization problem (3.23), without information on the distance geometries from Alice to Bob and Alice to Eve, there is no explicit solution. However

an optimal τ_B^* solution can be found for a given ϵ_T constraint and fixed $d_{A,B}$ as a function of varying $d_{A,E}$, as shown in Table 3.1. This case offers insight into a solution we can use for the two-hop case.

$d_{A,E}$	τ_B^*	T_p
2	7.6	$4.67 * 10^{-5}$
4	3.0	0.0156
9	1.5	0.1599
16	1.1	0.3835
25	0.9	0.6162
49	0.7	1.0346
100	0.5	1.5210
1000	0.4	2.6250

Table 3.1: Ranges of SNR yield different optimal τ_B^*; hence there is not a single τ_B^* that optimizes the throughput function.

Further, to maximize the end-to-end throughput of the two-hop network, the secrecy rates between the source-to-relay link and the relay-to-destination link, these secrecy rates should be equivalent or as close to as possible so that the network is not bottleneck. In other words, the network is limited by its weakest link; therefore, the links rates should be equalized, thus reducing the optimization problem:

$$\max \quad e^{-\tau_{B_1}} \left(R_{B_1} - R_{E_1}\right) = e^{-\tau_{B_2}} \left(R_{B_2} - R_{E_2}\right) \tag{3.24}$$

$$\text{s.t.} \quad \tau_{E_1} = \tau_{B_1} - \log_2(\epsilon_1)$$

$$\tau_{E_2} = \tau_{B_2} - \log_2(\epsilon_T - \epsilon_1) \tag{3.25}$$

where, following from the single-hop case, an optimal $\tau_{B_1}^*$ solution can be found for a given ϵ_T constraint and fixed $d_{A,B}$ as a function of varying $d_{A,E}$. For the two-hop case described above, the following algorithm then solves the optimization problem:

Algorithm 1 Find the optimal $(\epsilon_1^*, \epsilon_2^*)$, and (T_{P1}, T_{P2})

- Initialize the transmit SNR.
- Initialize the probability of outage constraint.

for varying Alice to Eve distance (d_{A,E_1}) on the first link **do**
  for varying relay to Eve distance (d_{A,E_2}) on the second link **do**
    - Partition the probability of outage constraint equally on each link.
    - Binary Search for the optimal probability of intercept constraint given the system settings.
    for varying ϵ_1, ϵ_2 **do**
      if $T_{P_1} = T_{P_2}$ **then**
        - the optimal end-to-end throughput is found, corresponding to the optimal $\epsilon_1^*, \epsilon_2^*$.
      else
        - Recursively call the binary search function.
      end if
    end for
  end for
end for

In Algorithm 1, we first initialize the end-to-end intercept probability constraint (ϵ_T), equally split the intercept probability constraint by link 1 (ϵ_1) and the intercept probability constraint by link 2 (ϵ_2) to $\frac{\epsilon_T}{2}$, and the transmit SNR $\left(\frac{E_S}{N_0}\right)$ is set to the desired power. Next for each distance geometry of the transmitter to eavesdropper pair (d_{A,E_1}, d_{A,E_2}), we find the optimal $\tau_{B_i}^*$, and T_{P_i} via a binary search on ϵ_i to satisfy the condition $T_{P_1} = T_{P_2}$ or, if at the end of the search, the value recorded corresponds to the optimal ($\min(T_{P_1}, T_{P_2})$) end-to-end throughput. Fig. 3.17 shows the end-to-end secure throughput for varying distances of two eavesdroppers away from the source where we find the optimal eavesdropper intercept constraint on each link (ϵ_1,ϵ_2) following Algorithm 1. Consider the case of the intercept probability constraint on each link are equal ($\epsilon_1 = \epsilon_2$). In Fig 3.18, the eavesdropper location of the first link is fixed at distance 1.41 units away from the source, while the location of the second eavesdropper is vary at a distance between $6.40 - 10.05$ units away from the transmitting relay node. As the second eavesdropper gets further away from the relay node, using an equality end-to-end intercept prob-

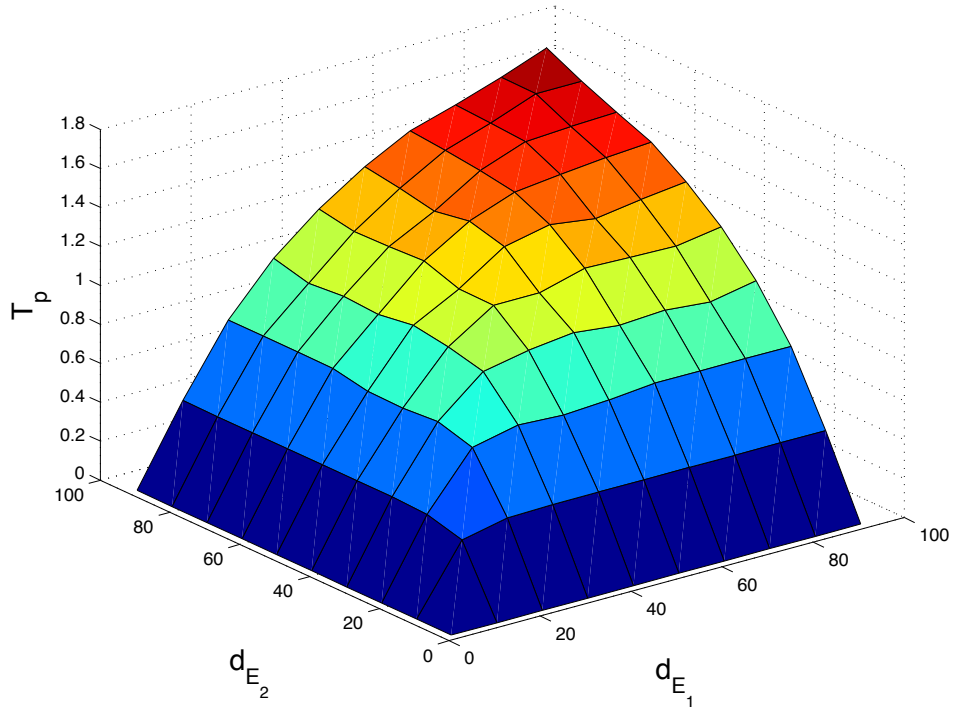


Figure 3.17: The maximum throughput is plotted versus varying eavesdropper distances (d_{E_1}, d_{E_2}) with the transmit SNR fixed at 20 dB, path-loss exponent of 2. The maximum throughput is found using the algorithm 1 discussed. The point at which the end-to-end throughput is maximized is when both eavesdroppers are farthest away from transmitting nodes. This figure can serve as a database to the achievable throughput given a pair of eavesdropper locations.

ability constraint ($\epsilon_1 = \epsilon_2$) has a damaging affect on throughput in comparison to the aforementioned two-hop optimal end-to-end constraint. We conclude that when the eavesdroppers distance from the transmitting nodes are unequal on both links, our end-to-end constraint leads to an increase in the end-to-end throughput. In other words if the eavesdroppers are at unequal distances from a transmitter node, a more relaxed intercept constraint should be place on that corresponding link ("trouble link"), while on the other hand, if an eavesdropper is further away from the source, the intercept constraint should be strict.

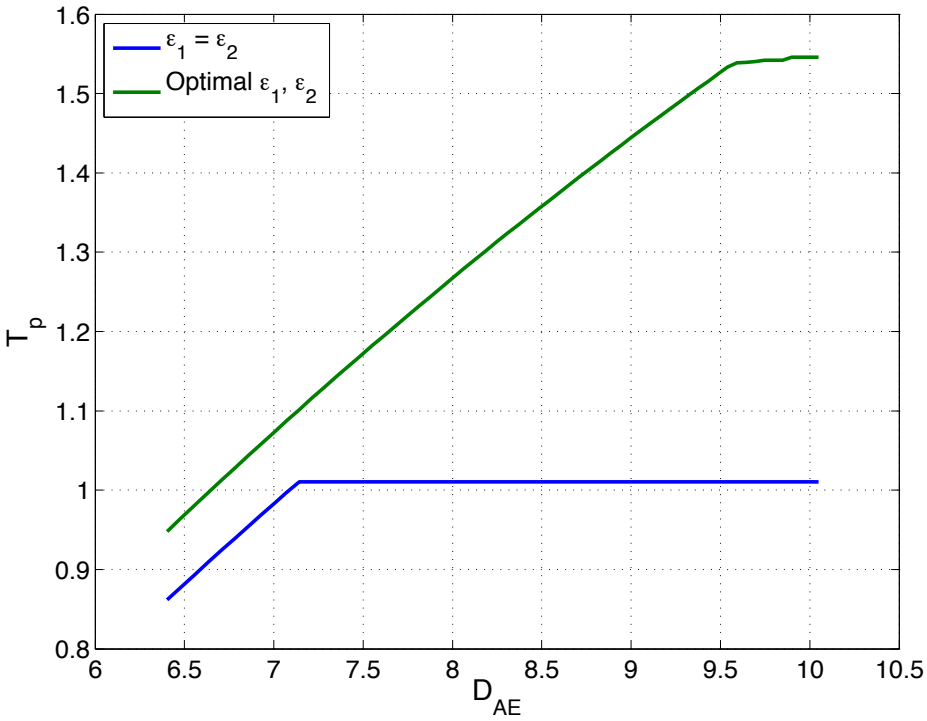


Figure 3.18: The maximum throughput is plotted for a fixed eavesdropper located 1.4 units away from the source versus a varying eavesdropper distance from the relay ($6.40 - 10.05$). The transmit SNR is fixed at 20 dB, the path-loss exponent is 2, and the total intercept probability constraint (ϵ_T) is 0.01. Comparison of our end-to-end constraint algorithm to an equal outage constraint on each link is shown. Partitioning using our end-to-end constraint (i.e. allocating intercept constraint to "trouble" link increases the secrecy rate) can achieve 55% increase in secure throughput.

3.6 Conclusion

Physical layer security is vital to wireless communications, and secrecy outage is an important measure of the reliability of a scheme. We first considered secrecy outage for the standard method, which, when channel state information is unavailable at the transmitter: (1) ignores the fact that it is not possible to build a universal wiretap code to cover the whole secrecy region required; and (2) treats all types of outage equitably. Next, a new outage formulation was presented where we consider rate pair design under the outage constraint, maintaining separate

rate thresholds for the channels to each of the destination (Bob) and eavesdropper (Eve). The new secrecy rate pair formulation reveals two unsecured regions for the standard formulation and motivates the application of hybrid ARQ to achieve secrecy. We design such an ARQ scheme to maximize throughput to Bob while constraining the intercept probability at Eve, while accounting for her ability to intercept the packet on the first or any retransmission (or, in the case of soft combining, some combination of the initial transmission and retransmissions). Numerical results are provided that demonstrate the utility of the definition and the significant secrecy rate improvements that can be obtained through the hybrid ARQ approach. Soft combining at the eavesdropper reduces the reliable secure throughput somewhat, but even much of this loss can be recouped if the legitimate receiver also employs soft combining. Later in the Chapter we extended our ARQ work to the two-hop case where we optimally solved for the best intercept constraint by eavesdroppers on the first and second link given an end-to-end intercept constraint. This resulted in an algorithm that favors allocating most of the intercept constraint to the "trouble link", i.e. the link where the eavesdropper is close to the transmitter.

In summary, information-theoretic security has shown many advantages over traditional cryptographic security. However information-theoretic security generally requires an advantage of the main channel over the eavesdropper channel. In the work described in this Chapter, the advantage came from the exploitation of the ubiquitous randomness in the wireless channel; fading. A weakness in this solution is the case when the eavesdropper is close to the source in which case minimal to null secrecy rate is achievable. In the next Chapter we will discuss a solution used to alleviate the near eavesdropper case.

CHAPTER 4

POWER ALLOCATION TO NOISE-GENERATING NODES FOR COOPERATIVE SECRECY IN THE WIRELESS ENVIRONMENT

The wireless transmission environment opens up opportunities for an eavesdropper to intercept a secret message from the source to the legitimate destination, particularly in the case when the eavesdropper is close to the source. Cooperative jamming, where nodes that are inactive serve as noise-generating nodes to disrupt an eavesdropper, has recently been considered in wireless communication networks to improve secrecy in such scenarios. Here we consider optimal power allocation to these jamming nodes (termed "chatterers") in the case of an eavesdropper of known location. The optimal power allocation to the chatterer nodes is achieved via a form of *water-filling* that, as one would expect, favors nodes that are close to the eavesdropper but will not impact the message to the destination significantly, either because the chatterer is located at a large distance from the destination or because the chatterer's signal is significantly faded at the destination. Numerical results compare the performance of the system employing the optimal power allocation to the performance of lower overhead schemes that employ only a single jamming node.

4.1 Introduction

In modern wireless communication applications such as transmissions from laptops, cellular phones, and sensor networks, secrecy can be very difficult to obtain due to the properties of the wireless medium, where the signal range is not

readily physically constrained. In particular, a message between a sender Alice and receiver Bob can be intercepted and/or jammed by an eavesdropper Eve. This can be a challenging problem because of the range of locations for Eve as seen in Chapter 3; an eavesdropper close to the transmitter has a significant signal-to-noise ratio (SNR) advantage over a distant receiver for reception, and a jammer near the receiver has a significant SNR advantage over the transmitter that can be employed to disrupt communication.

The traditional method to obtain secrecy as discussed in Section 3.1.1 is cryptography. In summary cryptography assumes an eavesdropper can perfectly listen to the message but its computational abilities restrict it from correctly decoding the message; hence, eavesdroppers near the source are accounted, which is of great value in the wireless environment. However if an eavesdropper has infinite computational abilities or stores the message for later decryption, security might be compromised.

Recall from Chapter 3 that Shannon [22] presented secrecy from an information-theoretic and physical layer background where he first considered transmission over a noiseless channel. Shannon's work assumes the adversary has perfect reception of the message and infinite computational abilities. In this case, he concluded (quite negatively) that secrecy required a key as long as the message. In a continuation of Shannon's work, Wyner considered secrecy over a noisy channel and introduced the wiretap channel [13]. Wyner's main result was that, if the channel from the source to the eavesdropper is a degraded version of the channel from the source to the destination, then perfect secrecy is achievable. Perfect secrecy means the source can transmit a message to the destination confidentially with the eavesdropper obtaining no information about the message. But, if the channel from the source to the eavesdropper is better than the source to destination, then secrecy

may not be achievable, which can occur in wireless systems if the eavesdropper is close to the source (the "near eavesdropper" problem).

One solution offered to the near eavesdropper problem was noise forwarding [25], where relay nodes send dummy codewords independent of the source message to confuse the eavesdropper. Another solution offered was cooperative jamming [26], where nodes not used in the relay transmission of the message but in close proximity to the eavesdropper introduce artificial random noise to degrade the message received at the eavesdropper. Contrary to noise forwarding, cooperative jamming allows the relay to harm the eavesdropper more than it harms the receiver. In [26], it was shown that a non-zero rate of secrecy can be achieved regardless of the eavesdropper location. In [27], cooperative jamming techniques that introduce artificial noise are again used to achieve secrecy. A protocol is introduced where system nodes that are not employed as relay nodes and that have a bad channel to the receiver (and hence will not interfere significantly with the message transmission), transmit random noise to confuse the eavesdropper. Results show that perfect secrecy can be achieved with high probability for a large number of randomly located eavesdroppers in the asymptotic case of a large number of systems nodes.

In this chapter we consider a similar but more practical case with a finite number of nodes. Given channel state information between all pairs of system nodes, it is possible to keep the destination out of outage if the aggregate chatterer power impinging on the receiver is constrained. This forms a constraint on the chatterer power, and we then investigate the optimal allocation of this power budget to the noise generating nodes, which we call "chattering nodes", with the goal of maximally degrading the eavesdropper signal. More formally, we guarantee a desired signal-to-interference plus noise ratio (SINR) at the destination while maximizing the probability that the eavesdropper cannot meet its (often lower) SINR threshold.

The problem formulation leads to a traditional *water-filling* result, where we allot power to chatterer nodes that are close to the eavesdropper and far from the destination, or whose signal will be badly faded when it arrives at the destination.

The communication between the source-to-destination may not be reliable, or even more important an eavesdropper may have a high probability to intercept the message, in which case a relay node can introduce transmit or security diversity to help in the end-to-end secure communication. Thus, next we focus on the optimal reliability outage allocation for the source-to-relay and relay-to-destination link while minimizing the probability of intercept to Eve.

The remainder of this chapter is organized as follows. Section 4.2 introduces the system model and metrics. Section 4.3 considers the optimal allocation of power to the chatterers, establishes the water-filling result, provides simulations examples, and discussion. Section 4.4 considers the two-hop network and optimal power allocation to chatters optimizing the outage constraint to the source-to-relay and relay-to-destination link. Finally, Section 4.5 provides the conclusions.

4.2 System Model and Metrics

4.2.1 Model

We consider the two-dimensional (2-D) network shown in Fig. 4.1, where a source node S (Alice) wishes to communicate to a destination node D (Bob) in the presence of a passive eavesdropper node E (Eve). Also present are potential "chattering" nodes, $Ch_1, Ch_2, ...Ch_{n-1}$, also known as jammers, used to disrupt the reception of the signal by the eavesdropper. The i^{th} transmitted symbol of the source node S is denoted by $x_i^{(S)}$, and the i^{th} received symbol for the eavesdropper E and the destination node D will be denoted by $y_i^{(E)}$ and $y_i^{(D)}$ respectively. We assume frequency non-selective Rayleigh fading between each of the active transmitters and receivers, where $h_{A,B}$ is the multipath fading on a link from a

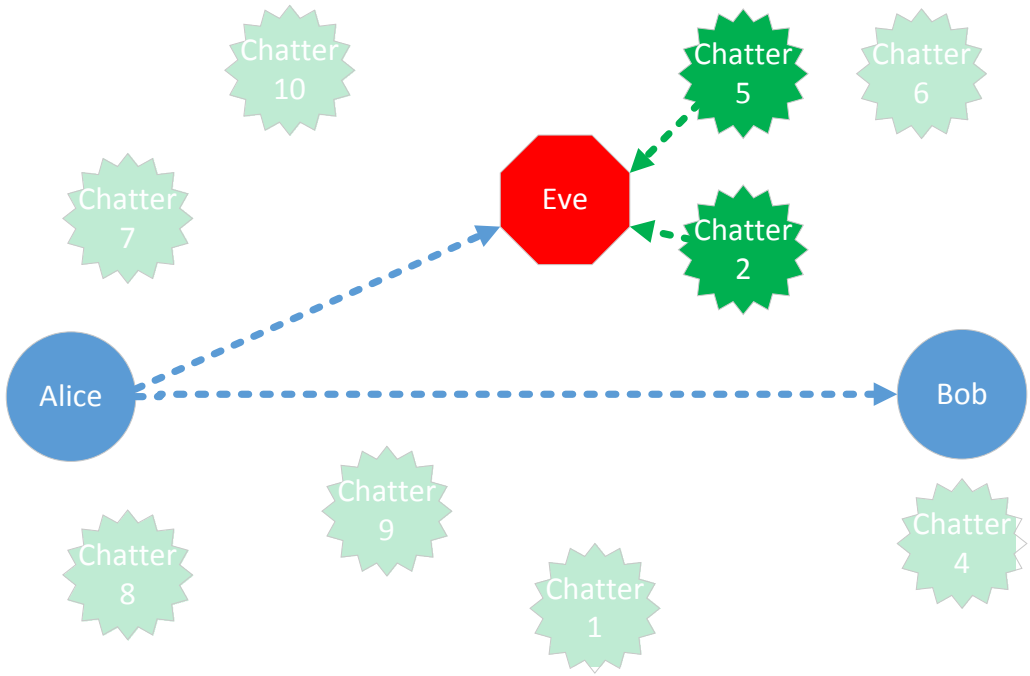


Figure 4.1: Alice attempting to secretly communicate to Bob (dashed blue arrow) in the presence of Eve and two chatter nodes (Chatter 2, Chatter 5) generating artificial noise to degrade Eve's received signal (green dashed lines).

given transmitter A to a given receiver B and is a complex zero-mean (complex) Gaussian random variable. The multipath fading is assumed to be constant over the duration of a codeword and independent for each distinct transmitter-receiver pair. The received signal at the eavesdropper and destination are, respectively:

$$\begin{aligned} y_i^{(E)} &= \frac{h_{S,E}}{\sqrt{d_{S,E}^{\alpha}}}\sqrt{E_s}x_i^{(S)} + n_i^{(E)} \\ y_i^{(D)} &= \frac{h_{S,D}}{\sqrt{d_{S,D}^{\alpha}}}\sqrt{E_s}x_i^{(S)} + n_i^{(D)} \end{aligned}$$

where E_s is the transmitted energy per symbol, $d_{A,B}$ is the distance between node A and B, α is the path-loss exponent, $n_i^{(E)}$ and $n_i^{(D)}$ are zero-mean Gaussian random variables with variance N_0, and, based on the Rayleigh fading assumption, $|h_{A,B}|^2$ is exponentially distributed with parameter 1. Throughout, we will assume that

the locations of all nodes, including that of the eavesdropper, are known, and that the channel gain $h_{A,B}$ for *system* nodes A and B is available (e.g. measured by pilots). Because of the assumption of a passive eavesdropper Eve, the value of $h_{S,E}$ is assumed to be unknown.

4.2.2 Metric

In this section we describe the metric on which the power optimization is based. The source S transmits the message to destination D, while the chatter nodes, Ch_1, Ch_2, ..., Ch_{n-1} transmit omnidirectional random Gaussian noise to create interference at the eavesdropper, E. Hence, conditioned on the channel fading gains, a Gaussian wiretap channel is obtained, whose instantaneous rate is given by

$$R = \log_2(1 + SINR_D) - \log_2(1 + SINR_E) \tag{4.1}$$

where $SINR_D$ and $SINR_E$ are the signal-to-interference plus noise ratios at the destination and eavesdropper, respectively, as given below. Now, suppose that we want to maintain a secrecy rate R_0 in our system. At first glance, it appears that one should design the system to maximize the probability that the ordered pair $(SINR_D, SINR_E)$ results in an R via (4.1) that is greater than R_0. However, given that a system would likely employ a single wiretap code in implementation, we consider a different approach.

Consider Figure 4.2. As discussed in detail in Chapter 3, whereas all ($SINR_D$, $SINR_E$) curves that lie below the $R = 2$ curve would satisfy the secrecy condition, there is not a single wiretap code that would be effective for all such cases. In particular, if one employs a wiretap code designed at (γ_D, γ_E), it will only be effective if both $SINR_D > \gamma_D$ and $SINR_E < \gamma_E$. Hence, rather than maximizing the probability of SINR rate pairs $(SINR_D, SINR_E)$ that result in an R via (4.1) that is greater than R_0, we consider constraints on both $SINR_D$ and $SINR_E$; in other words, we

consider a region given by one of the rectangles in Figure 4.2.

Since the channel state information is known for the channels between any pair of system nodes, it is possible to guarantee the desired SINR γ_D at the destination; that is, we will constrain:

$$SINR_D = \frac{\frac{|h_{S,D}|^2 P_s}{d_{S,D}^{\alpha}}}{\frac{N_0}{2} + \sum_{i=1}^{N} \frac{|h_{Ch_i,D}|^2 P_{Ch_i}}{d_{Ch_i,D}^{\alpha}}} = \gamma_D \tag{4.2}$$

where P_s is the amount of power transmitted by the source, and P_{Ch_i} is the power of the i^{th} chatter node. Likewise the (instantaneous) received $SINR$ at the eavesdropper is denoted as:

$$SINR_E = \frac{\frac{|h_{S,E}|^2 P_s}{d_{S,E}^{\alpha}}}{\frac{N_0}{2} + \sum_{i=1}^{N} \frac{|h_{Ch_i,E}|^2 P_{Ch_i}}{d_{Ch_i,E}^{\alpha}}} \tag{4.3}$$

In this case, $|h_{S,E}|^2$ is not known to the system, and thus $SINR_E < \gamma_E$ cannot be guaranteed. Thus, we instead seek to maximize the probability of this event. Hence, our optimization criterion is established: maximize eavesdropper outage $P(SINR_E < \gamma_E)$ given the destination receives the message successfully ($SINR_D = \gamma_D$).

4.3 Optimal Power Allocation

First, consider the intercept probability at Eve:

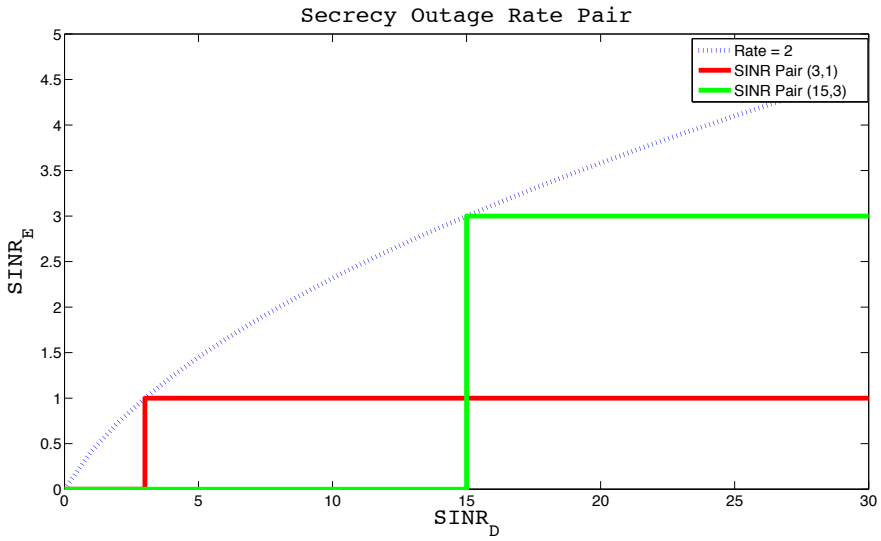


Figure 4.2: Secrecy curve of rate 2 is showed with dashed lines. The areas under the rectangles show the achievable regions of secrecy for two different codes.

$$
\begin{aligned}
P(SINR_E > \gamma_E) &= P\left(\frac{\frac{|h_{S,E}|^2 P_s}{d^\alpha_{S,E}}}{\frac{N_0}{2} + \sum_{i=1}^{N} \frac{|h_{Ch_i,E}|^2 P_{Ch_i}}{d^\alpha_{Ch_i,E}}} > \gamma_E\right) \\
&= E_{\{|h_{Ch_i,E}|^2, i=1,2,\ldots,N\}} \left[P\left(|h_{S,E}|^2 > \gamma_E \left(\frac{N_0}{2} + \sum_{i=1}^{N} \frac{|h_{Ch_i,E}|^2 P_{Ch_i}}{d^\alpha_{Ch_i,E}}\right)\left(\frac{d^\alpha_{S,E}}{P_s}\right)\right)\right] \\
&= E_{\{|h_{Ch_i,E}|^2, i=1,2,\ldots,N\}} \left[e^{-\left(\frac{N_0}{2} + \sum_{i=1}^{N} \frac{|h_{Ch_i,E}|^2 P_{Ch_i}}{d^\alpha_{Ch_i,E}}\right)\left(\frac{\gamma_E d^\alpha_{S,E}}{P_s}\right)}\right] \\
&= M \cdot E_{\{|h_{Ch_i,E}|^2, i=1,2,\ldots,N\}} \left[e^{-\gamma_E \sum_{i=1}^{N} \frac{|h_{Ch_i,E}|^2 P_{Ch_i}}{d^\alpha_{Ch_i,E}} \frac{d^\alpha_{S,E}}{P_s}}\right] \\
&= M \cdot \prod_{i=1}^{N} E_{|h_{Ch_i,E}|^2} \left[e^{-\gamma_E \frac{|h_{Ch_i,E}|^2 P_{Ch_i}}{d^\alpha_{Ch_i,E}} \frac{d^\alpha_{S,E}}{P_s}}\right] \\
&= M \cdot \prod_{i=1}^{N} \frac{1}{1 + \frac{P_{Ch_i}}{d^\alpha_{Ch_i,E}} \frac{d^\alpha_{S,E}}{P_s} \gamma_E}
\end{aligned} \tag{4.4}
$$

where $M = e^{-\gamma_E \frac{N_0}{2} \frac{d^\alpha_{S,E}}{P_s}}$ is the intercept probability without chatter. Our motive is to minimize (4.4), which is equivalent to minimizing the log of (4.4).

$$\min_{P_{Ch_i}} \quad \gamma_E \frac{N_0}{2} \frac{d^\alpha_{S,E}}{P_s} - \sum_{i=1}^{N} \ln\left(1 + \frac{P_{Ch_i}}{d^\alpha_{Ch_i,E}} \frac{d^\alpha_{S,E}}{P_s} \gamma_E\right) \tag{4.5}$$

$$\text{s.t.} \quad \frac{\frac{|h_{S,D}|^2 P_s}{d^\alpha_{S,D}}}{\frac{N_0}{2} + \sum_{i=1}^{N} \frac{|h_{Ch_i,D}|^2 P_{Ch_i}}{d^\alpha_{Ch_i,D}}} = \gamma_D, \quad P_{Ch_i} \geq 0, i = 1, 2, ..., N \tag{4.6}$$

The first constraint implies:

$$\sum_{i=1}^{N} \frac{|h_{Ch_i,D}|^2 P_{Ch_i}}{d^\alpha_{Ch_i,D}} = \frac{|h_{S,D}|^2 P_s}{d^\alpha_{S,D} \gamma_D} - \frac{N_0}{2} \tag{4.7}$$

Now, define

$$\widetilde{P}_{Ch_i} = P_{Ch_i} \frac{|h_{Ch_i,D}|^2}{d^\alpha_{Ch_i,D}} \tag{4.8}$$

Then, the problem is:

$$\max_{\widetilde{P}_{Ch_i}} \quad \sum_{i=1}^{N} \ln\left(1 + \frac{d^\alpha_{Ch_i,D}}{d^\alpha_{Ch_i,E}} \frac{d^\alpha_{S,E}}{|h_{Ch_i,D}|^2 P_s} \widetilde{P}_{Ch_i} \gamma_E\right) \tag{4.9}$$

$$\text{s.t.} \quad \sum_{i=1}^{N} \widetilde{P}_{Ch_i} = \frac{|h_{S,D}|^2 P_s}{d^\alpha_{S,D} \gamma_D} - \frac{N_0}{2}, \widetilde{P}_{Ch_i} \geq 0, i = 1, 2, ...N \tag{4.10}$$

Therefore the solution that maximizes capacity is a similar result to that for parallel Gaussian channels:

$$\widetilde{P}_{Ch_i} = (r - N_i)^+ = \begin{cases} (r - N_i), & \text{if } r - N_i \geq 0 \\ 0, & \text{if } r - N_i < 0 \end{cases} \tag{4.11}$$

where in our optimization problem N_i is equivalent to $\frac{|h_{Ch_i,D}|^2 P_s d^\alpha_{Ch_i,E}}{d^\alpha_{S,E} d^\alpha_{Ch_i,D} \gamma_E}$. Thus, the power is distributed via *water-filling* [55] and then (4.8) is used to find the chatterer

power. In other words chatterers that are geometrically, very close to an eavesdropper and far away from the destination together with having a bad fade to the destination will be allocated the most power. This should match our intuition since we desire to maximally decrease the eavesdropper intercept probability (i.e. chatter close to an eavesdropper) together with not interfering with the source-to-destination communication (i.e. chatter far from and bad fade to the destination).

4.3.1 Toy Example

Fig. 4.3 shows the performance of the scenario that consists of a Alice, Bob, and Eve with 5 system nodes. In this example we considered γ_D as fixed at 10 dB, while an eavesdropper intercepts the packet if it is above the lower threshold $\gamma_E = 5$ dB. Also, the 5 system nodes are placed at 4 different geometries for 0, 1, 5, and a random number of chatter nodes placed close to an eavesdropper, as summarized in Table 4.1. As described in the previous section, the power distribution to system nodes follows the *water-filling* algorithm, allocating power to system nodes that degrade the eavesdropper ability to intercept a message while minimally affecting the source-to-destination communication. Also in Table 4.1 we highlight some of the key parameters captured in the toy example. First, in the case where we have a random set of system nodes or $N = 1$ system node close to Eve yields approximately the same intercept probability by Eve. We see that when 5 system nodes are placed close to Eve, that we see $\approx 85\%$ reduction in intercept probability. The intercept values by Eve for the other cases, e.g. when $N = 5$ system nodes are not close to Eve are unsatisfactory. As will be explained in more detail in Section 4.3.3, we can heavily reduce the intercept probability by Eve, by allowing outage (not transmit) at the destination when the intercept probability by Eve is above a threshold. Fig. 4.4 shows the intercept probability by Eve performance as a function of the

amount of outage we allow to the destination. We can see there is significant gain employing the aforementioned scheme.

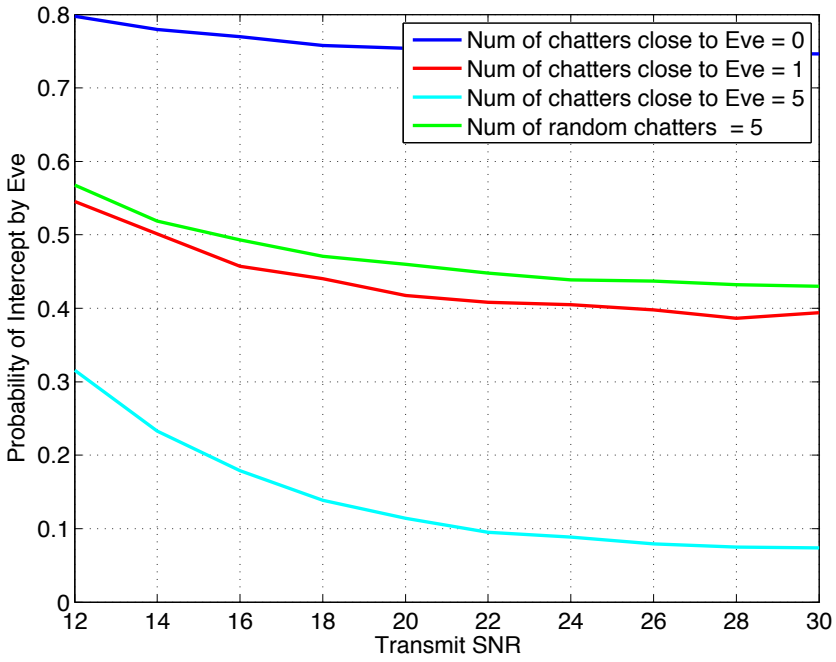


Figure 4.3: Probability of intercept of the message by Eve versus probability of outage for the destination, for $N = 5$ system nodes present with a transmit SNR of 20 dB, and Alice, Eve, and Bob are fixed at $(0.0, 0.50)$, $(0.20, 0.20)$, $(1.00, 0.50)$ respectively. There different scenarios are considered, $N = 5, 3, 1$ system nodes are close to the eavesdropper and $N = 5$ randomly present system nodes. The pathloss exponent is set to $\alpha = 2$, the required SINR at the destination is set to $\gamma_D = 10$, and the required SINR at the eavesdropper is set to $\gamma_E = 5$. Each data point is the result of 10,000 trials. For each trial, the optimal chattering computed, and the eavesdropper intercept probability is calculated. The eavesdropper intercept probability is averaged over those trials when the system was not in outage

4.3.2 Set Up

The wireless scenario considered is shown in Figure 4.5. The wireless link operates on the region $[0, 1] \times [0, 1]$, with the source located on the left side at coordinates $(0.00, 0.50)$ and the destination on the right side at coordinates $(1.00, 0.50)$. In between are N system nodes and an eavesdropper, all of which are uniformly dis-

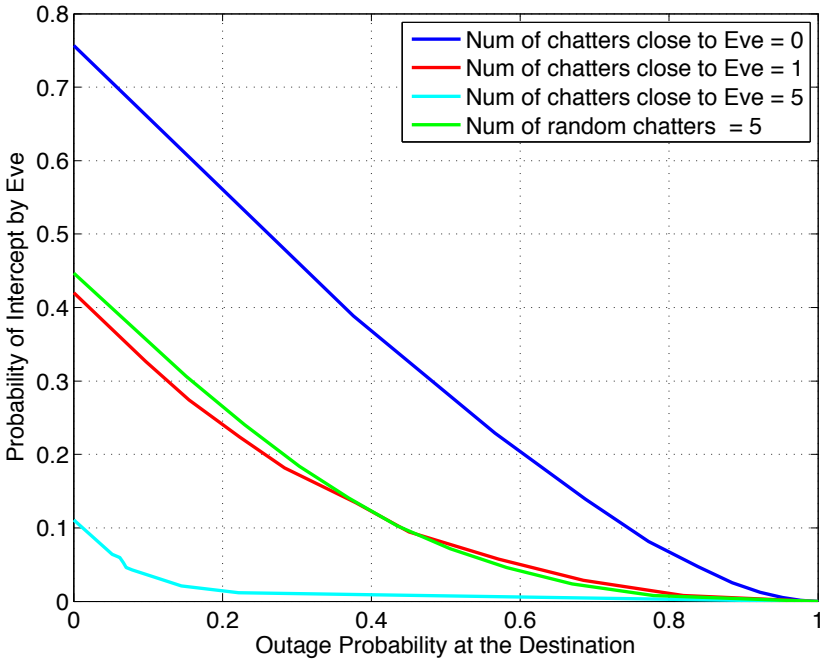


Figure 4.4: Probability of intercept of the message by Eve versus probability of outage for the destination, for $N = 5$ system nodes present with a transmit SNR of 20 dB, and Alice, Eve, and Bob are fixed at $(0.00, 0.50)$, $(0.20, 0.20)$, $(1.00, 0.50)$ respectively. There different scenarios are considered, $N = 5, 3, 1$ system nodes are close to the eavesdropper and $N = 5$ randomly present system nodes. The pathloss exponent is set to $\alpha = 2$, the required SINR at the destination is set to $\gamma_D = 10$, and the required SINR at the eavesdropper is set to $\gamma_E = 5$. Each data point is the result of 10,000 trials. For each trial, the optimal chattering computed, and the eavesdropper intercept probability is calculated. Then, per the text, the system employs its knowledge of this eavesdropper intercept probability to decide when the eavesdropper intercept probability will be too high and accepts an outage for the destination in those situations. The eavesdropper intercept probability is averaged over those trials when the system was not in outage

tributed at random across the region. Note that this scenario emphasizes the near eavesdropper problem, since the eavesdropper will likely be closer to the source than the destination. The parameters of the system are set as follows: the pathloss exponent is set to $\alpha = 2$, the required SINR at the destination is set to $\gamma_D = 10$, the required SINR at the eavesdropper (which we want to insure the received SINR is less than) is set to $\gamma_E = 5$. The ratio of the transmit power P_s to N_0, which we

Nodes close to Eve	γ_1	Chatter Locations	P_{int}
5	0.00	$(0.25, 0.25)$, $(0.15, 0.15)$, $(0.30, 0.30)$,$(0.01, .10)$,$(0.20, 0.30)$	0.11
5	0.30	$(0.25, 0.25)$, $(0.15, 0.15)$, $(0.30, 0.30)$,$(0.01, .10)$,$(0.20, 0.30)$	0.01
1	0.00	$(0.80, 0.80)$, $(0.75, 0.75)$, $(0.50, 0.50)$,$(0.40, .80)$,$(0.30, 0.30)$	0.42
1	0.30	$(0.80, 0.80)$, $(0.75, 0.75)$, $(0.50, 0.50)$,$(0.40, .80)$,$(0.30, 0.30)$	0.17
0	0.00	$(0.80, 0.80)$, $(0.75, 0.75)$, $(0.50, 0.50)$,$(0.40, .80)$,$(1.00, 0.10)$	0.75
0	0.30	$(0.80, 0.80)$, $(0.75, 0.75)$, $(0.50, 0.50)$,$(0.40, .80)$,$(1.00, 0.10)$	0.46
Random	0.00	random	0.46
Random	0.30	random	0.19

Table 4.1: Alice, Bob and Eve are fixed at $(0.00, 0.50)$,$(1.00, 0.50)$, and $(0.20, 0.20)$ respectively. Transmit SNR is set to 20 dB. The required SINR is set to 10 dB at the destination and the eavesdropper intercepts the packet if its SINR is above the threshold 5 dB. Probability of intercept by Eve is show for 4 different scenarios: $N = 0, 1, 5$, and random number of nodes are placed close to the eavesdropper. Also, considered is the case of allowing outage by Bob and the corresponding security performance.

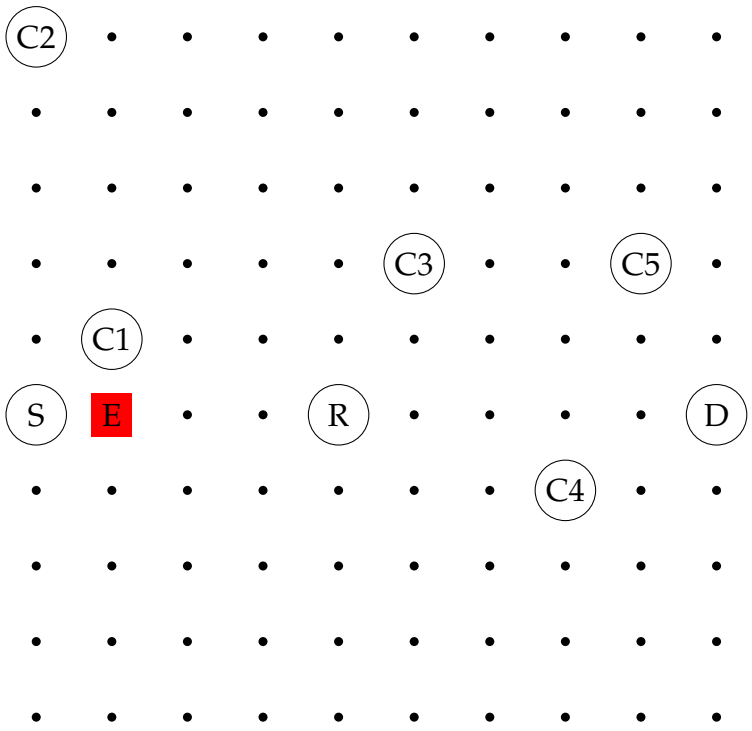


Figure 4.5: Two-Dimensional (2-D) scenario where the source, and destination are located at $(0.00, 0.50)$, $(1.00, 0.50)$ respectively. Also, 5 system nodes are randomly placed which can possibly serve as chatter nodes.

will call the "transmit SNR", will be varied as the independent variable. Since the path-loss between the source and destination is always fixed at one, this will also

be the average received SNR. We will vary the transmit SNR from just above γ_D to much higher values. Although the eavesdropper also benefits from a higher transmit power, larger gaps between the transmit SNR and γ_D allow us to introduce more chatter to thwart the eavesdropper until saturation occurs, as observed and discussed below.

The simulation runs as follows. For each trial, the N system nodes and the eavesdropper E are randomly placed. Next, the (independent) fading values between all pairs of nodes are randomly generated. Recall that the location of the eavesdropper is known to the system, and the fading value between any pair of *system* nodes is assumed known, but the fading value for any link between a system node and the eavesdropper is unknown. The constraint on the chatterer powers such that γ_D is met at the destination is then calculated, and then *water-filling* as described in the previous section is employed to find $\tilde{P}_{Ch_i}, i = 1, 2, \ldots, N$, which then leads directly to the chatterer powers $P_{Ch_i}, i = 1, 2, \ldots, N$. The chatterer powers are then used to calculate the probability that the eavesdropper is in outage. This latter is averaged over the trials to produce the eavesdropper outage probability. We employed 10,000 trials for each simulation point unless otherwise noted.

4.3.3 Results

First, consider the difficulty of the near eavesdropper problem using simple one-way wireless transmission without any chattering. For this, we ran the system shown in Figure 4.5 with $N = 0$ (no system nodes except the source and destination) with the parameters given above with a transmit SNR ranging from 13 to 30 dB. We found that the eavesdropper is unlikely to be in outage, with a probability of outage starting at around 5% at 13.0 dB and decreasing with further increasing transmit SNR, as expected; hence, the message is nearly always intercepted by the eavesdropper. Next, we added N chatterers to the system and repeated the ex-

periment for $N = 3, 10, 20$, and 50 using the power setting derived in this work. The results are shown in Figure 4.6. Note that the results are relatively invariant to SNR, as expected. Although the SNR at the destination without chatter needs to be higher than γ_D to allow some chatter, increasing the transmit SNR also makes it easier for the eavesdropper to intercept the message and performance eventually saturates.

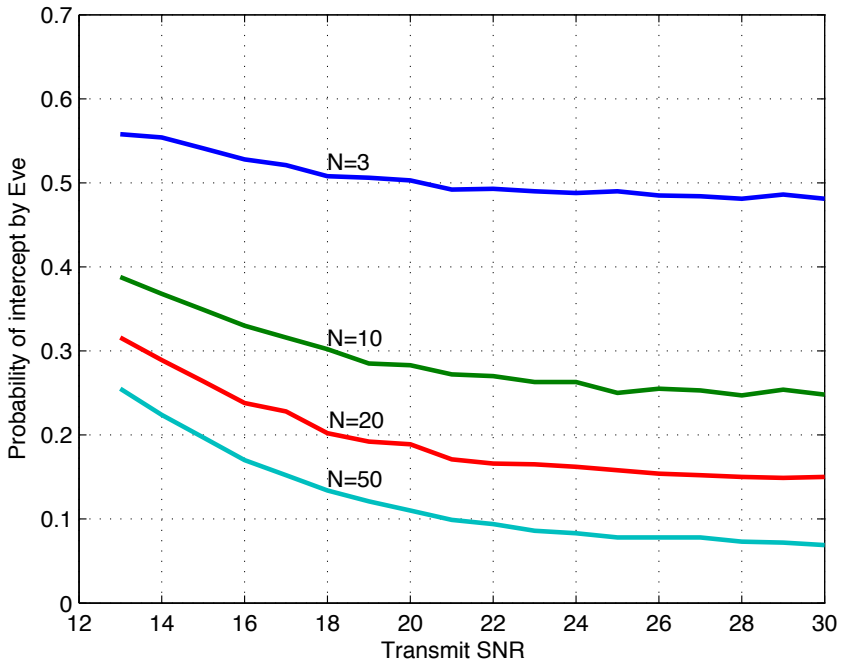


Figure 4.6: Probability of intercept of the message by Eve versus transmit SNR when N system nodes are present in the system for the scenario of Figure 4.5. The pathloss exponent is set to $\alpha = 2$, the required SINR at the destination is set to $\gamma_D = 10$, and the required SINR at the eavesdropper is set to $\gamma_E = 5$. Each data point is the result of 10,000 trials. For each trial, the nodes are randomly placed, the optimal chattering computed, and the eavesdropper intercept probability is calculated. The result shown is the average of the eavesdropper intercept probability over all trials.

The results shown in Figure 4.6 are not satisfactory, as even a large number of potential chatterers ($N = 50$) and a large transmit SNR does not lead to a very secure system with only a probability of intercept slightly less than 10%, which would be unacceptable in practice. However, from the simulations, we notice that

the intercept probability is dominated by a few bad geometries and fading situations. In other words, occasionally: (1) the eavesdropper is right near the source, or (2) the source to destination link experiences severe multipath fading, which allows for almost no chattering. In fact, the intercept probability at the eavesdropper can be quite close to one in some situations. However, note that, given its knowledge of the location of the eavesdropper and the chatterer power employed, the system is able to calculate $P(SINR_E > \gamma_E)$ while operating. In practice, the system could simply not transmit when $P(SINR_E > \gamma_E)$ is larger than an acceptable threshold. This would lead to the potential for outage for the destination, but hopefully at a significantly decreased probability of intercept for the eavesdropper. The results from such an exercise are shown in Figure 4.7. As expected, the eavesdropper intercept probability drops rapidly as we allow some outage at the destination. Hence, if there is no delay constraint and nodes are mobile the destination can significantly reduce the probability that a packet is intercepted by the eavesdropper with a mild reduction in data rate.

Finally, with the goal of simplifying the implementation, we consider a scheme where only a single node chatters. There are multiple possibilities here. For example, one could have the node closest to the eavesdropper chatter, which would not require the transmission of channel state information as the fading evolves. However, a more effective method is to increase the power of the relay, that, after the *waterfilling* allocation of power to $P_{Ch_i}, i = 1, 2, \ldots, N$, has the largest impact on the eavesdropper outage, which is equivalent to selecting the relay with the largest $P_{Ch_i}/d^{\alpha}_{Ch_i,E}$. We hasten to note that this is not necessarily the optimal selection of a single node for chattering but will give us an idea of how closely the use of a single node can approach the optimal use of all nodes. The results are shown in Figure 4.8. Comparing Figures 4.6 and 4.8, we see that the loss from employing only a

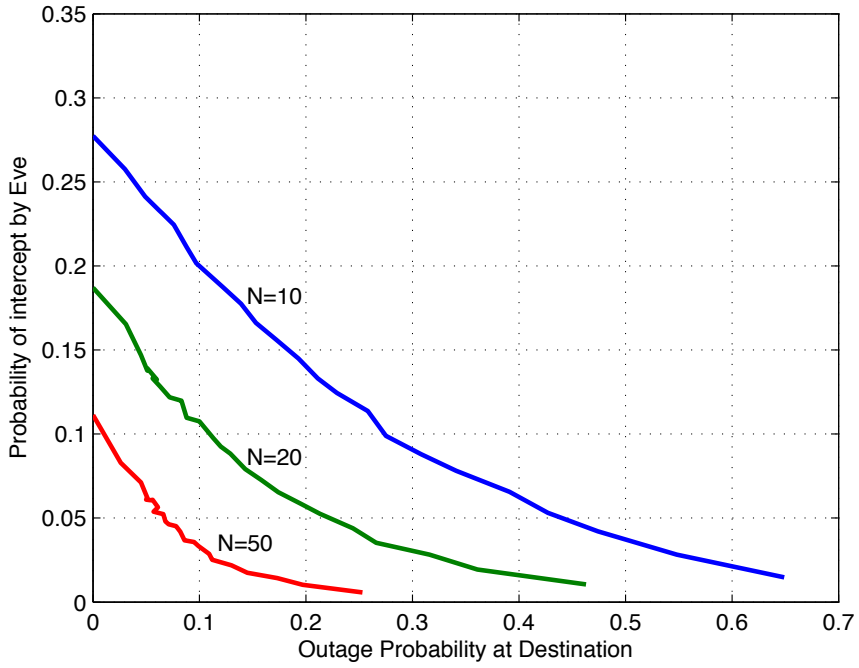


Figure 4.7: Probability of intercept of the message by Eve versus probability of outage for the destination, for $N = 10$, $N = 20$ and $N = 50$ system nodes present with a transmit SNR of 20 dB. The pathloss exponent is set to $\alpha = 2$, the required SINR at the destination is set to $\gamma_D = 10$, and the required SINR at the eavesdropper is set to $\gamma_E = 5$. Each data point is the result of 10,000 trials. For each trial, the nodes are randomly placed, the optimal chattering computed, and the eavesdropper intercept probability is calculated. Then, per the text, the system employs its knowledge of this eavesdropper intercept probability to decide when the eavesdropper intercept probability will be too high and accepts an outage for the destination in those situations. The eavesdropper intercept probability is averaged over those trials when the system was not in outage.

single well-chosen node is often small, particularly when only a small number of system nodes are available.

4.4 Two-hop Network

Communication is not always widely available between the source and destination. In this case a relay node is needed to assist in the end-to-end communication. Relay node helps with wireless diversity and reliability of the message to the

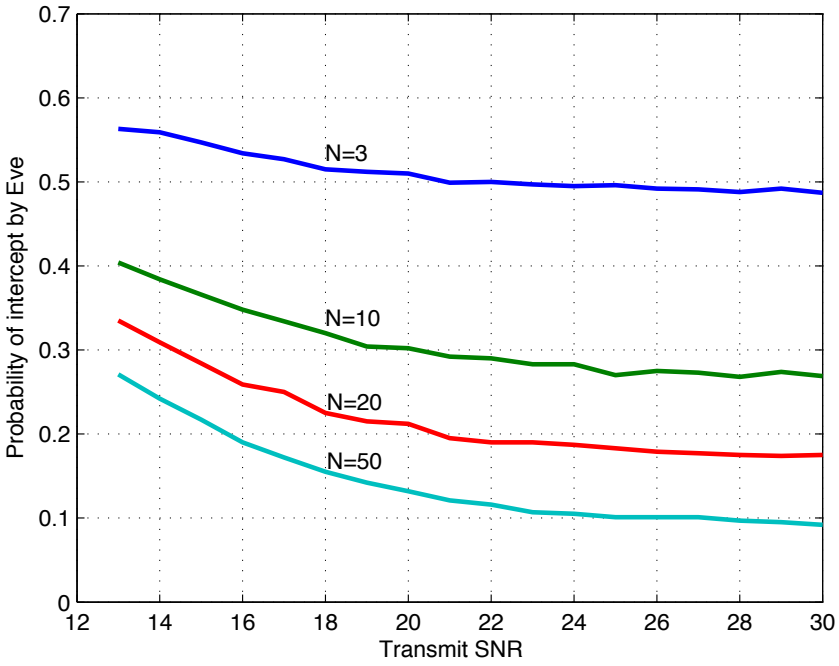


Figure 4.8: Probability of intercept of the message by Eve versus transmit SNR when N system nodes are present in the system for the scenario of Figure 4.5, but with only a single node producing chatter. The pathloss exponent is set to $\alpha = 2$, the required SINR at the destination is set to $\gamma_D = 10$, and the required SINR at the eavesdropper is set to $\gamma_E = 5$. Each data point is the result of 10,000 trials. For each trial, the nodes are randomly placed and the optimal chattering computed. Then, the node with the largest impact on the eavesdropper intercept probability is allocated all of the power (i.e. including that it was not allocated before) so that only a single node chatters. The results shown are the average of the eavesdropper intercept probability over all trials.

destination. We consider a two-hop network where the source communicates to the destination via a relay, and an eavesdropper listens to two independent transmission attempts to maliciously intercept the message. As explained earlier in this section, chatter nodes will be used to aid in the secrecy while maintaining the desired reliability of the message. Under these circumstances we seek to find the optimal allocation of the end-to-end total reliability constraint on the source-to-relay link and relay-to-destination link that minimizes the end-to-end probability of intercept by Eve. Similarly to earlier work, we introduce a fixed outage to each

link to further minimize the probability of intercept by Eve, but, choose the optimal outage to each link. First Recall :

$$SINR_{E_j} = \frac{|h_{S,E_j}|^2 P_S}{d^{\alpha}_{S,E_j}\left(\frac{N_0}{2} + \sum_{i=1}^{N} \frac{|h_{Ch_i,E_j}|^2 P_{Ch_i}}{d^{\alpha}_{Ch_i,E_j}}\right)} \tag{4.12}$$

for $i = 1, 2$, where $SINR_{E_1}$, $SINR_{E_2}$ is the independent SINR received at the eavesdropper from the first and second transmission respectively.

$$SINR_{B_j} = \frac{|h_{S,B_j}|^2 P_S}{d^{\alpha}_{S,B_j}\left(\frac{N_0}{2} + \sum_{i=1}^{N} \frac{|h_{Ch_i,B_j}|^2 P_{Ch_i}}{d^{\alpha}_{Ch_i,B_j}}\right)} \tag{4.13}$$

for $i = 1, 2$, where $SINR_{B_1}$,$SINR_{B_2}$, is the SINR constraint at the relay and destination respectively.

Consider the probability of secrecy outage due to Eve intercepting the message:

$$\begin{aligned} P(I) &= P(I_1 \cup I_2) = P(I_1) + P(I_2) - P(I_1 \cap I_2) \\ &= P(I_1) + P(I_2) - P(I_1)P(I_2) \\ &\approx P\left(SINR_{E_1} > \gamma_E\right) + P\left(SINR_{E_2} > \gamma_E\right) \end{aligned} \tag{4.14}$$

where (4.14) used the fact that the the eavesdropper intercept probability on each link is independent, and the end-to-end intercept probability is the union of the intercept on the first and second transmission. Similarly to the result in Section 4.3, we get:

$$e^{-\frac{d_{S,E_1}\gamma_E N_0}{2P_S}} \prod_{i=1}^{N} \frac{1}{1 + \frac{P_{Ch_i} d^{\alpha}_{S,E_1}\gamma_E}{P_S d^{\alpha}_{Ch_i,E_1}}} + e^{-\frac{d_{S,E_2}\gamma_E N_0}{2P_S}} \prod_{i=1}^{N} \frac{1}{1 + \frac{P_{Ch_i} d^{\alpha}_{S,E_2}\gamma_E}{P_S d^{\alpha}_{Ch_i,E_2}}} \tag{4.15}$$

The optimization problem is the following:

$$\max_{\widetilde{P}_{Ch_i}} \quad \sum_{i=1}^{N} \ln\left(1 + \frac{d^{\alpha}_{Ch_i,B_j}}{d^{\alpha}_{Ch_i,E_j}} \frac{d^{\alpha}_{S,E_j}}{|h_{Ch_i,B_j}|^2 P_S} \widetilde{P}_{Ch_i} \gamma_E\right) \tag{4.16}$$

$$\text{s.t.} \quad \sum_{i=1}^{N} \widetilde{P}_{Ch_i} = \frac{|h_{S,B_j}|^2 P_S}{d^{\alpha}_{S,B_j} \gamma_{B_j}} - \frac{N_0}{2}, \widetilde{P}_{Ch_i} \geq 0, i = 1, 2, ...N \tag{4.17}$$

where $\widetilde{P}_{Ch_i} = \frac{P_{Ch_i}|h_{Ch_i,B_i}|^2}{d_{Ch_i,B_j}}$. Similarly to the single hop case, leads to *water-filling* solution:

$$\widetilde{P}_{Ch_i} = (r - N_{j,i})^+ = \begin{cases} (r - N_{j,i}), & \text{if } r - N_{j,i} \geq 0 \\ 0, & \text{if } r - N_{j,i} < 0 \end{cases} \tag{4.18}$$

$$N_{j,i} = \frac{|h_{Ch_i,B_j}|^2 P_S d^{\alpha}_{Ch_i,E_j}}{d^{\alpha}_{S,E_j} d^{\alpha}_{Ch_i,B_j} \gamma_E} \tag{4.19}$$

We saw from the earlier Section 4.3 that allowing for outage at the legitimate receiver leads to significant gain in minimizing the probability of intercept at the eavesdropper. The optimization problem will determine the optimal outage to the relay (link 1) and destination (link 2) such that we minimize the end-to-end probability of intercept. In the next section we will discuss the algorithm used and simulation results for the aforementioned optimization problem.

4.4.1 Set Up

The wireless scenario considered is shown in Figure 4.9. The wireless link operates on the region $[0, 1] \times [0, 1]$, with the source located on the left side at coordinates $(0.00, 0.50)$, the relay in the middle at coordinates $(0.50, 0.50)$, and the destination on the right side at coordinates $(1.00, 0.50)$. In between are N system nodes and an eavesdropper, all of which are placed at random across the region. As explained earlier in the chapter, this scenario emphasizes the near eavesdropper

problem, since the eavesdropper will likely be closer to the source than the destination. The parameters of the system are set as follows: the pathloss exponent is set to $\alpha = 2$, the required SINR at the relay and destination is set to $\gamma_{B_j} = 10$, the required SINR at the eavesdropper is set to $\gamma_E = 5$. The "transmit SNR" is fixed at 20 dB.

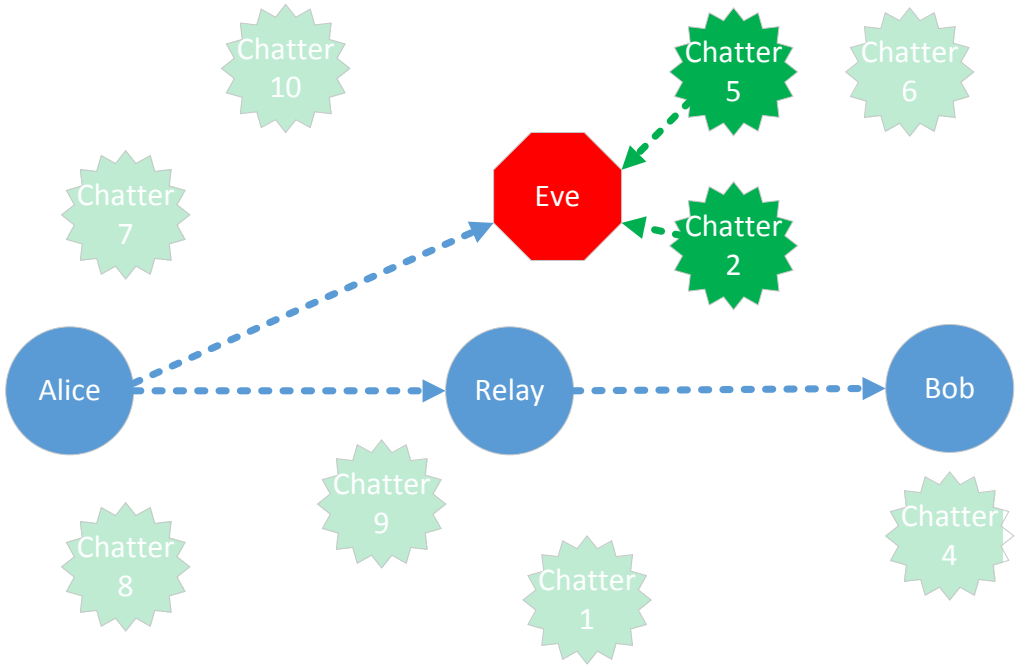
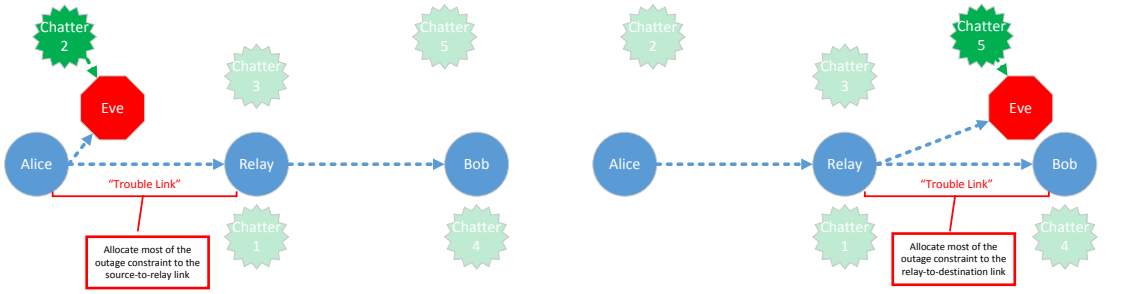


Figure 4.9: Alice communicates to Bob via a Relay node in the presence of Eve. Also in the environment are 10 system nodes of which Chatter 2 and Chatter 5 mostly contribute artificial noise to disrupt the eavesdropper while having minimal effect on the two hop transmission.

We will consider two different toy examples to illustrate the importance on choosing the optimal reliability outage constraint to the relay and destination, γ_1, and γ_2 respectively. In the first example Fig. 4.10a, the eavesdropper is fixed at position $(0.01, 0.50)$, extremely close to the source, one of the most vulnerable regions in the system. In the next example, Fig. 4.10b, we consider the eavesdropper fixed extremely close to the destination at $(0.99, 0.50)$. These toy examples show how

the performance with an optimal choice of γ_1, γ_2 compares to the performance if we had just decided to allocate $\gamma_1 = \gamma_2$.



(a) Toy Example 1: Eve extremely close to the source.

(b) Toy Example 2: Eve extremely close to the destination.

Figure 4.10: These two examples show two different cases where outage is mostly allocated to the trouble link.

To figure out the optimal source-to-relay outage (γ_1) and relay-to-destination outage (γ_2), minimizing the end-to-end intercept probability of the eavesdropper, we used the following Algorithm:

Algorithm 2 Find the optimal transmitter-receiver outage constraint (γ_1, γ_2).

- Initialize γ_T.
- Initialize γ_1, γ_2 to add up to γ_T.

for each $\gamma_1 < \gamma_T$ **do**

- *water-fill* on link 1 and record the optimal probability of intercept to Eve ($P_{int}^{(1)}$).
- *water-fill* on link 2 and record the optimal probability of intercept to Eve ($P_{int}^{(2)}$).
- Add the end-to-end intercept probability ($P_{int}^{(T)} = P_{int}^{(1)} + P_{int}^{(2)}$).

end for

Return $\min(P_{int}^{(T)}) \leftarrow \gamma_1^*, \gamma_2^*$

4.4.2 Results

Very important in the two-hop scenario is the link on which the eavesdropper has a higher probability of intercepting a message. If the eavesdropper location is

unknown or equally far from the source and relay, then its best to allocate the outage to the legitimate receivers equally as shown in Fig. 4.11. However in the case when the eavesdropper favors one link then its very important to allocate more outage to the " trouble link". To highlight the significance of outage allocation to the available links lets consider the toy examples set up from Section 4.4.1.

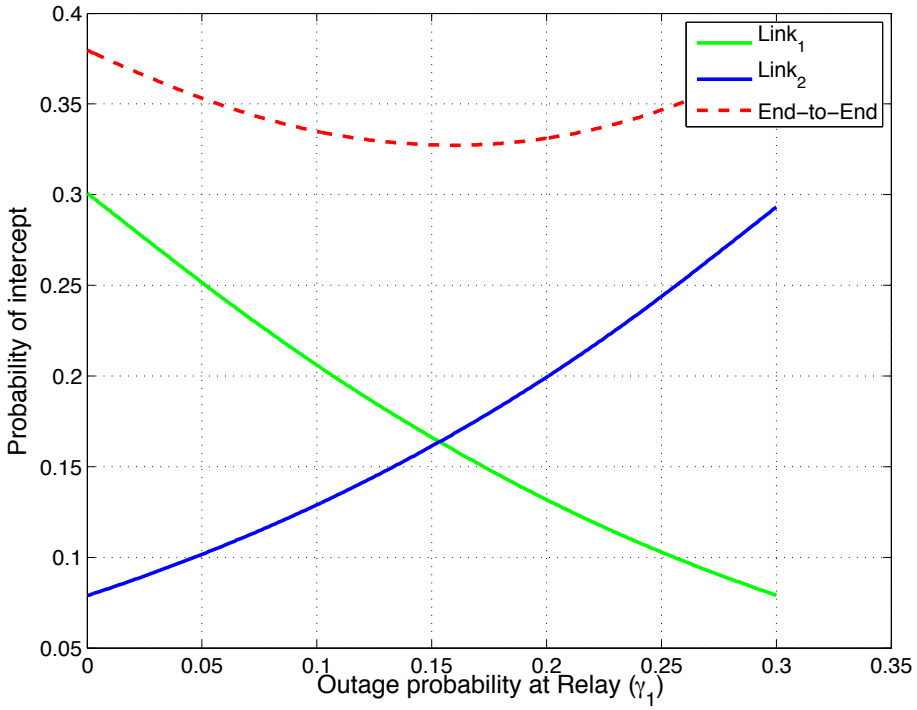


Figure 4.11: Alice, relay, Bob, and Eve are placed at the fixed coordinates $(0.00, 0.50)$, $(0.50, 0.50)$, $(1.00, 0.50)$, $(0.99, 0.50)$ as shown in Fig. 4.11. Considered the case of $N = 10$ system nodes for $10,000$ iterations, the probability of intercept by Eve is averaged for various γ_1, where $\gamma_T = 0.3$, and $\gamma_2 = \gamma_T - \gamma_1$. The eavesdropper is a major security threat to $link_2$, therefore it is very desirable to allocate most of the outage to γ_2 to minimize the end-to-end probability of intercept.

Consider the performance of toy example #1; Fig. 4.12. Recall that the source, relay and the destination are located at coordinates $(0.00, 0.50)$, $(0.50, 0.50)$, and $(1.00, 0.50)$ respectively. The eavesdropper is placed particularly close to the source, which represents an extremely vulnerable state for the first hop, link 1. On the

other hand because the eavesdropper is very far away geometrically from link 2, the probability of intercept is significantly less probable; low security concern. Since the goal is to minimize the probability of intercept by the eavesdropper, given the freedom to choose the probability of outage (reliability) on link 1 and link 2, γ_1 should receive a large allocation of the outage constraint in order to minimize the probability of intercept at the eavesdropper because of the high chance that the eavesdropper gets the message on the first hop. Similarly in Fig. 4.13 we consider the case where the eavesdropper was located extremely close to the destination, as a result majority of the outage allocation is given to γ_2 to minimize the end-to-end probability of intercept of the message.

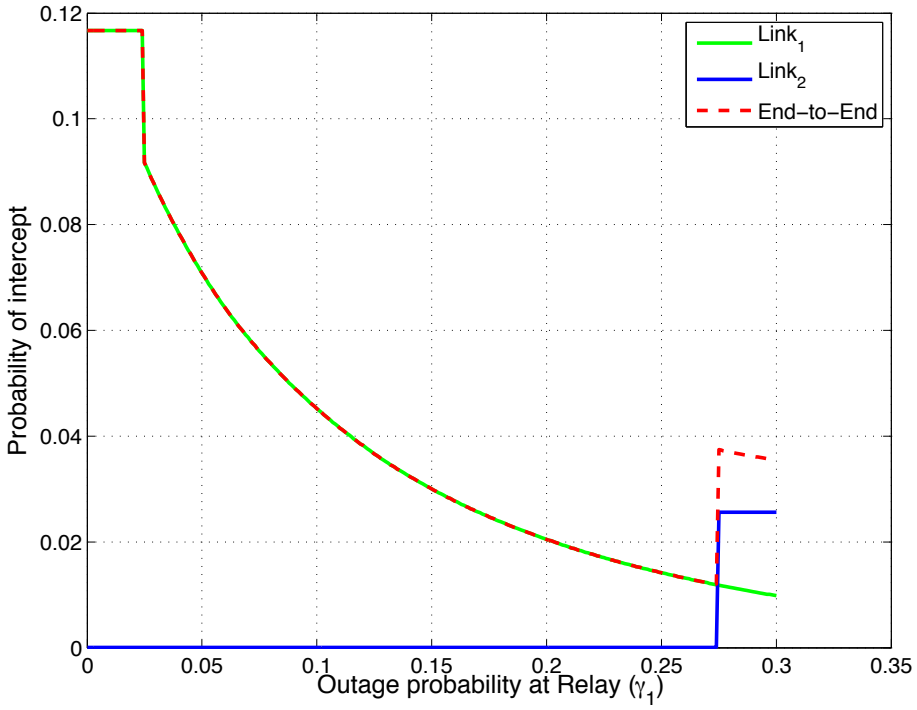


Figure 4.12: Alice, relay, Bob, and Eve are placed at the fixed coordinates $(0.00, 0.50)$, $(0.50, 0.50)$, $(1.00, 0.50)$, $(0.01, 0.50)$ as shown in Fig. 4.10a. Considered the case of $N = 10$ chatters for $10,000$ iterations, the probability of intercept by Eve is averaged for various γ_1, where $\gamma_T = 0.3$, and $\gamma_2 = \gamma_T - \gamma_1$. The eavesdropper is a major security threat to *link*1; therefore, it is very desirable to allocate most of the outage to γ_1 to minimize the probability of intercept.

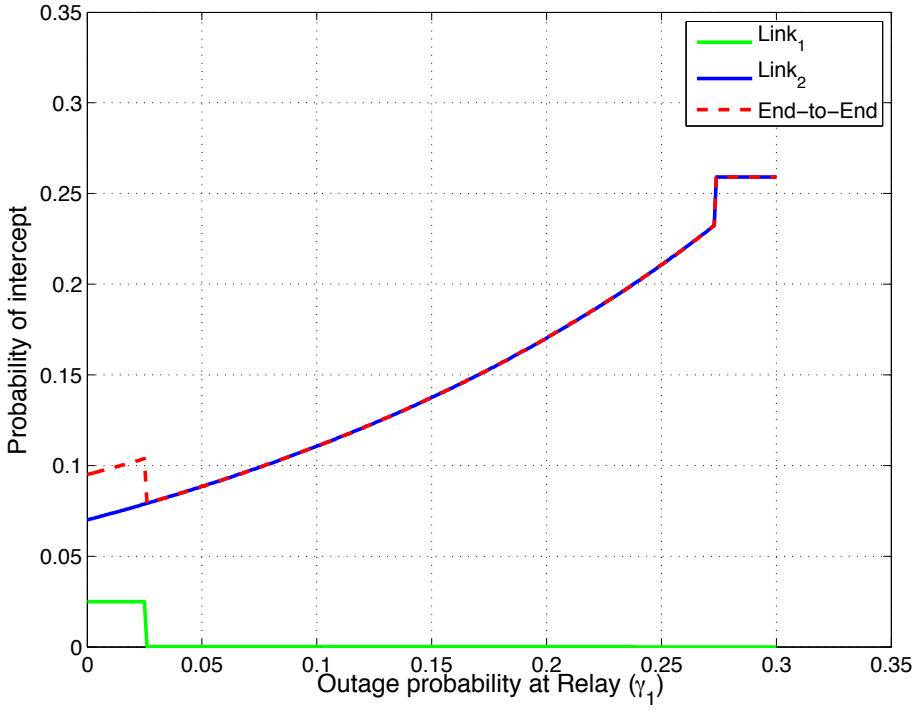


Figure 4.13: Source, relay, destination, and Eve are placed at the fixed coordinates $(0.0, 0.50), (0.50, 0.50), (1.00, 0.50), (0.99, 0.50)$ as shown in Fig. 4.10b. Considered the case of $N = 10$ system nodes, for $10,000$ iterations, the probability of intercept at Eve is averaged for various γ_1, where $\gamma_T = 0.3$, and $\gamma_2 = \gamma_T - \gamma_1$. The eavesdropper is a major security threat to $link_2$; therefore, it is very desirable to allocate most of the outage to γ_2 to minimize the probability of intercept.

These results are summarized in Table 4.2, where savings in the probability of intercept by Eve is shown using our approach in determining the optimal γ_1, γ_2 for each link in comparison to equally choosing γ_1 and γ_2. For the case of the eavesdropper being close to the source or the destination, we can reduce the probability of intercept by Eve by 60% and 42% respectively.

In Fig. 4.14, we consider the case of the end-to-end probability of intercept savings by Eve as a function of Eve distance from the source for a moderately dense network ($N = 20$) and dense network ($N = 50$). The most savings is achieved when Eve is either close to the source or close to the destination, mainly because

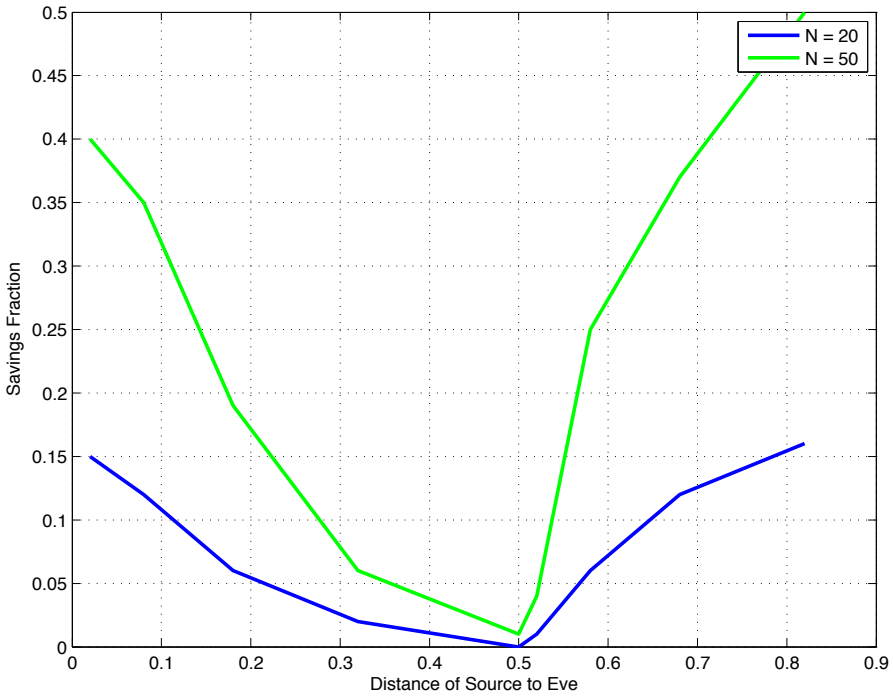


Figure 4.14: Alice, relay, and Bob are placed at the fixed coordinates $(0.0, 0.50)$, $(0.50, 0.50)$, $(1.00, 0.50)$. Considered the case of $N = 20$ and $N = 0$ system nodes, for $10,000$ iterations, savings in the probability of intercept by Eve in our optimal outage allocation for γ_1, γ_2 in comparison to equal outage allocation ($\gamma_1 = \gamma_2$), as a function of the distance from Alice to Eve. When Eve is either very close to the source or furthest away from the source yields the most savings. On the other hand, when Eve is equally away from Alice as it is from the Relay, equal outage allocation is optimal since the eavesdropper does not favor a link.

that is when Eve favors a particular link. The savings decreases as the coordinate changes from 0.1 to 0.5 because Eve is approaching closer to the relay node. Whereas as the coordinate changes from 0.5 to 1.0 Eve is getting further away from the relay.

4.5 Conclusion

Communication between a source and destination in the presence of a passive eavesdropper is considered. System nodes other than the source and destina-

Scenario	$P_{int}^{(T)^*}$	γ_1^*	γ_2^*	Savings
Close to Source	0.0120	0.2740	0.0260	60%
Close to Destination	0.0792	0.0260	0.2740	42%

Table 4.2: This table shows the optimal end-to-end intercept probabilities with corresponding receiver outage constraints on link 1 (γ_1) and link 2 (γ_2) for the toy problems described when the number of system nodes, $N = 10$. The last column is the savings in the intercept probability for the optimal (γ_1, γ_2) in comparison to if the outage constraint was equally split for both links. There is significant gain for carefully selecting γ_1, γ_2 as described.

tion generate random chatter to aid in the secret transmission of the message. In contrast to maintaining a pair of received signal-to-noise-plus-interference ratios (SINR) such that the secrecy rate equation is satisfied, we argue that maintaining separate SINR thresholds at the receiver and eavesdropper will be required if a single wiretap code is employed. This naturally leads to a formulation where the SINR threshold at the receiver is met with equality, while the probability that the SINR threshold is met at the eavesdropper is maximized. With an appropriate change of variables, optimal power allocation to the systems nodes that generate random chatter can be achieved via a water-filling approach. Numerical results indicate that, even with this optimum power allocation, the eavesdropping probability is intolerably high if zero outage must be maintained at the receiver. Hence, we consider allowing a small outage at the receiver, which greatly reduces the eavesdropping probability. We note that allocating power to only a single chattering node often does not result in a significant reduction in performance versus the optimal allocation. Lastly, we considered the two-hop network, figuring out the optimal outage constraint to each link given an end-to-end outage constraint. Importantly, we defined the "trouble link" as a link that had an eavesdropper with a high probability to intercept the message, e.g. as a result of being close to a transmitting node. For this case it was shown that there is significant gain in secrecy

performance using our outage allocation scheme rather than equally partitioning the outage to each link.

CHAPTER 5

CONCLUSION

In this dissertation we have considered two main areas of concern in wireless communications: wideband receiver design and security. We first studied ultra-wideband (UWB), a promising communications technique that helps resolve the frequency allocation problem that often inhibits narrowband systems. We unified reference-based noncoherent receivers into one general framework for performance evaluation to consider the optimal set of waveforms under various constraints and the comparison of the prominent systems. We contributed sample-and-hold techniques and halving the frequency offset to optimize Frequency Shifted Reference (FSR-UWB) to improve performance in the case of an average power constraint. Next we optimized multi-data rate systems that faced a peak power constraint by applying a novel form of tone reservation. The latter contribution is different than traditional tone reservation seen in orthogonal frequency division multiplexing (OFDM) because peak reducing "dummy" carriers are added above the coherence frequency, thus not sacrificing data rate or system performance.

We also have considered the important topic of security in wireless communications. Most modern wireless systems use cryptography, which typically relies on a secret key shared by trusted parities and complex algorithms to hide a message from an eavesdropper. However, in this dissertation we have considered information-theoretic approaches because they guarantee everlasting security. We considered the selection of code parameters for the case of communication from Alice (the transmitter) to Bob (the intended recipient) in the presence of Eve (an

eavesdropper) when all channels experience multipath fading whose values are not known at the transmitter. In particular we provided a new secrecy outage formulation, where rather than only define secrecy outage with one degree of freedom, the target secrecy rate threshold as in the standard formulation, we defined secrecy outage as an individual rate pair with two degrees of freedom. In the construction of the new outage formulation, we noted that two secrecy outage regions emerged that violated the secrecy rate pair outage formulation but were not equal in consequence. In the first event, the target secrecy rate was met but the eavesdropper and destination rates were higher than the designed wiretap code, which is disastrous because the eavesdropper intercepts the packet: the system is insecure. In the other event, the instantaneous rates of the eavesdropper and the destination channels are lower than the designed wiretap code but we can exploit the use of automatic retransmission (ARQ) while maintaining the intercept probability of the eavesdropper below the desired threshold. We then introduced a sophisticated hybrid ARQ receiver, where a buffer was used to combine incomplete packets from previous transmissions to improve reliability. Secrecy with hybrid ARQ showed good system performance, especially as the eavesdropper distance from the source increased. Next, the two-hop case was considered where the goal was to determine the secrecy rate pair on each link with the corresponding intercept probability constraints given only the end-to-end intercept probability constraint. We contributed a binary search algorithm to efficiently find the optimal rate pairs on both links for various intercept probability constraints to result in the maximum end-to-end throughput.

Last, motivated by the weakness of secrecy with ARQ in certain scenarios the near eavesdropper case was investigated. We considered the power allocation to nearby "chatter" nodes that amplify artificial noise to disrupt the eavesdropper but not significantly affect the SINR of the main communication. This contribu-

tion resulted in a *water-filling* approach, where we put power into nodes that had a good fade and close distance to the eavesdropper while being far away and having a bad fade to the destination. Under some circumstances this resulted in an unsatisfactory intercept probability of Eve, which we improved by allowing outage at the destination to significantly reduce the intercept probability to Eve. Later we extended this work to the two-hop case, with an end-to-end outage constraint. We optimized the outage allocated to each link and showed that the outage constraint should be budgeted to the "trouble link" to maximize secrecy performance.

APPENDIX A

NOISE ANALYSIS OF UNIFIED FRAMEWORK

In this appendix, the second moments of the "signal cross noise" term in (2.12) are evaluated.

$$\int_0^{T_s} \sum_{K=0}^{K-1} \phi_k^2(t)\phi_f^2(t)dt \tag{A.1}$$

Noise Cross Noise Analysis:

$$\begin{aligned}
& E[(\int_0^{T_s} n^2(t)\phi_k(t))^2] \\
\overset{(1)}{=} & \int_0^{T_s}\int_0^{T_s} E[n(t)n(t)n(s)n(s)]\phi_k(t)\phi_k(s)dsdt \\
= & R_n^2(0)\int_0^{T_s}\phi_k(t)dt\int_0^{T_s}\phi_k(s)ds + 2\int_0^{T_s}\int_0^{T_s} R_n^2(s-t)\phi_k(t)\phi_k(s)dsdt \\
= & 2\int_0^{T_s}\int_0^{T_s} R_n^2(s-t)\phi_k(t)\phi_k(s)dsdt \\
\overset{(2)}{=} & T_s N_0^2 W
\end{aligned} \tag{A.2}$$

where $R_n(\tau)$ denotes the autocorrelation function of the wideband noise process $n(t)$, $\overset{(1)}{=}$ comes from the standard decomposition of the expectation of the product of four Gaussian random variables, and $\overset{(2)}{=}$ comes from Parsevals Theorem. Signal Cross Noise Analysis:

$$
\begin{aligned}
& E[(2\int_0^{T_s} x(t)n(t)\phi_k(t)dt)^2] \\
= \;& 4\int_0^{T_s}\int_0^{T_s} x(t)x(s)R_n(t-s)\phi_k(t)\phi_k(s)dsdt \\
\overset{(1)}{=} \;& 4\int_0^{T_s}\int_0^{T_s} u(t)u(s)R_n(t-s)\phi_k(t)\phi_k(s)dsdt \\
\overset{(2)}{\approx} \;& 4\sum_{n=0}^{N_f-1} x_{env}^2(t)(nT_f)\phi_k^2(nT_f)\int_0^{T_s} p(t-nT_f)p(s-nT_f)R_n(t-s)dsdt \\
\overset{(3)}{\approx} \;& \frac{2N_0}{T_s}\int_0^{T_s} x_{env}^2(t)(t)\phi_k^2(t)dt \\
= \;& \frac{2N_0}{T_s}\int_0^{T_s}[\sqrt{E_r}u(t)+\sum_{m=0}^{K-1}(-1)^{b_0^{(m)}}\sqrt{E_d^{(m)}}\phi_m(t)u(t)]^2\phi_k^2(t)dt \qquad \text{(A.3)}
\end{aligned}
$$

where $\overset{(1)}{=}$ follows because the support of $R_n(\tau)$, is far less than $T_f - T_p$, $\overset{(2)}{=}$ and $\overset{(3)}{=}$ follow because of the limited support of the autocorrelation function $R_n()$ of the wideband process $n(t)$. For simplification we evaluate the above integral in (A.3) term by term:

$$
\frac{2N_0E_r}{T_s}\int_0^{T_s}\phi_k^2(t)dt = 2E_rN_0 \qquad \text{(A.4)}
$$

$$
\frac{2N_0}{T_s}\int_0^{T_s}\sum_{m=0}^{K-1} b_0^{(m)}\sqrt{E_rE_d^{(m)}}\phi_m(t)\phi_k^2(t)dt = 0 \qquad \text{(A.5)}
$$

$$
\begin{aligned}
& \frac{2N_0}{T_s}\int_0^{T_s}\sum_{m=0}^{K-1}(b_0^{(m)})^2E_d^{(m)}\phi_m^2(t)\phi_k^2(t)dt \\
& +\frac{2N_0}{T_s}\int_0^{T_s}\sum_{m=0}^{K-1}\sum_{m\neq n}^{K-1} b_0^{(m)}b_0^{(n)}\sqrt{E_d^{(m)}E_d^{(n)}}\phi_m(t)\phi_n(t)\phi_k^2(t)dt \qquad \text{(A.6)}
\end{aligned}
$$

APPENDIX B

NECESSITY CONDITIONS FOR SECRECY WITH ARQ (TWO-HOP CASE)

The method of Lagrange multipliers is introduced to maximize the overall secrecy throughput of the end-to-end path while constraining the total end-to-end intercept probability (secrecy with ARQ two-hop optimization problem):

$$\max_{\tau_{Ei},\tau_{Bi}} f(\tau_{Ei},\tau_{Bi}) = (1-e^{-\tau_{B_i}})\left[\log_2\left(\frac{P_s\tau_{B_i}+N_0 d_{S,B_i}^{\alpha}}{N_0 d_{S,B_i}^{\alpha}}\right)-\log_2\left(\frac{P_s\tau_{E_i}+N_0 d_{S,E_i}^{\alpha}}{N_0 d_{S,E_i}^{\alpha}}\right)\right]$$
$$\text{s.t.}\quad h(\tau_{Ei},\tau_{Bi}) = \sum_{i=1}^{2}\frac{e^{-\tau_{E_i}}}{1-(1-e^{-\tau_{B_i}})(1-e^{-\tau_{E_i}})} = \epsilon_T \tag{B.1}$$

Set the derivations $\bigtriangledown F(\tau_{E_j},\tau_{B_j}) + \lambda \bigtriangledown H(\tau_{E_j},\tau_{B_j}) = 0$, which yields the system of equations (necessity conditions) below respectively:

$$-\left(e^{-\tau_{B_j}}\left[\log_2\left(\frac{P_s\tau_{B_j}+N_0 d_{S,B_j}^{\alpha}}{N_0 d_{S,B_j}^{\alpha}}\right)-\log_2\left(\frac{P_s\tau_{E_j}+N_0 d_{S,E_j}^{\alpha}}{N_0 d_{S,E_j}^{\alpha}}\right)\right]+\left(1-e^{-\tau_{B_j}}\right)\frac{P_s}{P_s\tau_{B_j}+N_0 d_{S,B_j}^{\alpha}}\right) = \lambda\left(\frac{-e^{-\tau_{E_j}}(e^{-\tau_{E_j}}e^{-\tau_{B_j}}-e^{-\tau_{B_j}})}{(e^{-\tau_{B_j}}+e^{-\tau_{E_j}}-e^{-\tau_{E_j}}e^{-\tau_{B_j}})^2}\right) \tag{B.2}$$

$$\left(1-e^{-\tau_{B_j}}\right)\frac{P_s}{P_s\tau_{E_j}+N_0 d_{S,E_j}^{\alpha}} = \lambda\left(\frac{-e^{-\tau_{E_j}}(-e^{-\tau_{E_j}}+e^{-\tau_{E_j}}e^{-\tau_{B_j}})}{(e^{-\tau_{B_j}}+e^{-\tau_{E_j}}-e^{-\tau_{E_j}}e^{-\tau_{B_j}})^2} - \frac{e^{-\tau_{E_j}}}{(e^{-\tau_{E_j}}+e^{-\tau_{B_j}}-e^{-\tau_{E_j}}e^{-\tau_{B_j}})}\right) \tag{B.3}$$

$$\frac{e^{-\tau_{E_j}}}{e^{-\tau_{E_j}}+e^{-\tau_{B_j}}-e^{-\tau_{E_j}}e^{-\tau_{B_j}}} - \epsilon_T = 0 \tag{B.4}$$

First solving (B.4) for τ_{E_j} yields :

$$
\begin{aligned}
e^{-\tau_{E_j}} &= \frac{\epsilon e^{-\tau_{B_j}}}{1-\epsilon+\epsilon e^{-\tau_{B_j}}} \\
\tau_{E_j} &= \tau_{B_j} - \log_2 \frac{\epsilon}{1-\epsilon+\epsilon e^{-\tau_{B_j}}}
\end{aligned}
\tag{B.5}
$$

Next we substitute (B.5) into (B.3) where an analytical solution for τ_{B_j} could not be found.

BIBLIOGRAPHY

[1] "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area networks (WPANs)," *IEEE Standard 802.15.3*, pp. 1–315, 2003.

[2] A. F. Molisch, K. Balakrishnan, C. chin Chong, S. Emami, A. Fort, J. Karedal, J. Kunisch, H. Schantz, U. Schuster, and K. Siwiak, "IEEE 802.15.4a channel model - final report," in *Converging: Technology, work and learning. Australian Government Printing Service*, 2004.

[3] R. Wilson and R. Scholtz, "Comparison of CDMA and modulation schemes for UWB radio in a multipath environment," in *Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE*, vol. 2, 2003, pp. 754–758 Vol.2.

[4] R. Hoctor and H. Tomlinson, "Delay-hopped transmitted-reference RF communications," in *Ultra Wideband Systems and Technologies, 2002. Digest of Papers. 2002 IEEE Conference on*, 2002, pp. 265–269.

[5] D. Goeckel and Q. Zhang, "Slightly Frequency-Shifted Reference Ultra-Wideband (UWB) Radio," *Communications, IEEE Transactions on*, vol. 55, no. 3, pp. 508–519, 2007.

[6] Q. Zhang, D. Goeckel, J. Burkhart, B. Mui, N. Merrill, M. Carrier, and R. Jackson, "FSR-UWB (TR-UWB without the Delay Element): Effect of Impulse Dithering and Experimental Results," in *Ultra-Wideband, The 2006 IEEE 2006 International Conference on*, 2006, pp. 315–320.

[7] D. Goeckel, J. Mehlman, and J. Burkhart, "A Class of Ultra Wideband (UWB) Systems with Simple Receivers," in *Military Communications Conference, 2007. MILCOM 2007. IEEE*, 2007, pp. 1–7.

[8] H. Nie and Z. Chen, "Performance analysis of code-shifted reference UWB radio," in *Radio and Wireless Symposium, 2009. RWS '09. IEEE*, 2009, pp. 396–399.

[9] A. D'Amico and U. Mengali, "Code-multiplexed UWB transmitted-reference radio," *Communications, IEEE Transactions on*, vol. 56, no. 12, pp. 2125–2132, 2008.

[10] K. Morrison, C. Capar, Z. Lai, D. Goeckel, and R. Jackson, "A unified framework for reference-based ultra-wideband signaling," in *Ultra-Wideband, 2009. ICUWB 2009. IEEE International Conference on*, 2009, pp. 290–294.

[11] M. Bloch and J. Barros, *Physical-Layer Security*. Cambridge University Press, 2011.

[12] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels," in *Information Theory, 2006 IEEE International Symposium on*, 2006, pp. 356–360.

[13] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[14] S. Lin, D. Costello, and M. Miller, "Automatic-repeat-request error-control schemes," *Communications Magazine, IEEE*, vol. 22, no. 12, pp. 5–17, 1984.

[15] H. Sheng, R. You, and A. Haimonvich, "Performance analysis of ultra-wideband rake receivers with channel delay estimation errors," in *Information Sciences and Systems, 2004 IEEE Conference on.*, 2004.

[16] A. Batra, J. Balakrishnan, G. Aiello, J. Foerster, and A. Dabak, "Design of a multiband ofdm system for realistic UWB channel environments," *Microwave Theory and Techniques, IEEE Transactions on*, vol. 52, no. 9, pp. 2123–2138, 2004.

[17] M. R. Casu and G. Durisi, "Implementation aspects of a transmitted-reference UWB receiver," *Wireless Communications and Mobile Computing Journal*, vol. 5, pp. 537–549, aug 2005. [Online]. Available: http://www.nari.ee.ethz.ch/commth/pubs/p/wcmcj05

[18] N. Van Stralen, A. Dentinger, I. Welles, K., J. Gaus, R., R. Hoctor, and H. Tomlinson, "Delay hopped transmitted reference experimental results," in *Ultra Wideband Systems and Technologies, 2002. Digest of Papers. 2002 IEEE Conference on*, 2002, pp. 93–98.

[19] Q. Zhang and D. Goeckel, "Multi-Differential Slightly Frequency-Shifted Reference Ultra-wideband (UWB) Radio," in *Information Sciences and Systems, 2006 40th Annual Conference on*, 2006, pp. 615–620.

[20] J. Pagliery. (2014, May) Half of American adults hacked this year. [Online]. Available: http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/

[21] W. Diffie and M. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, 1976.

[22] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.

[23] Y. Liang, H. Poor, and S. Shamai, "Secure Communication Over Fading Channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2470–2492, 2008.

[24] P. K. Gopala, L. Lai, and H. El-Gamal, "On the Secrecy Capacity of Fading Channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 10, pp. 4687–4698, 2008.

[25] L. Lai and H. El Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy," *Information Theory, IEEE Transactions on*, vol. 54, no. 9, pp. 4005–4019, 2008.

[26] R. Negi and S. Goel, "Secret communication using artificial noise," in *In IEEE Vehicular Technology Conference*, 2005, pp. 1906–1910.

[27] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial Noise Generation from Cooperative Relays for Everlasting Secrecy in Two-Hop Wireless Networks," *Selected Areas in Communications, IEEE Journal on*, vol. 29, no. 10, pp. 2067–2076, 2011.

[28] H. Liu, A. Molisch, S. Shiwei Zhao, D. Goeckel, and P. Orlik, "Hybrid Coherent and Frequency-Shifted-Reference Ultrawideband Radio," in *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE*, 2007, pp. 4106–4111.

[29] Y.-L. Chao and R. Scholtz, "Optimal and suboptimal receivers for ultrawideband transmitted reference systems," in *Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE*, vol. 2, 2003, pp. 759–763 Vol.2.

[30] J. Choi and W. Stark, "Performance of ultra-wideband communications with suboptimal receivers in multipath channels," *Selected Areas in Communications, IEEE Journal on*, vol. 20, no. 9, pp. 1754–1766, 2002.

[31] S. Gezici, F. Tufvesson, and A. Molisch, "On the performance of transmitted-reference impulse radio," in *Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE*, vol. 5, 2004, pp. 2874–2879 Vol.5.

[32] T. Quek and M. Win, "Analysis of UWB transmitted-reference communication systems in dense multipath channels," *Selected Areas in Communications, IEEE Journal on*, vol. 23, no. 9, pp. 1863–1874, 2005.

[33] L. Yang and G. Giannakis, "Timing ultra-wideband signals with dirty templates," *Communications, IEEE Transactions on*, vol. 53, no. 11, pp. 1952–1963, 2005.

[34] Q. Zhang and D. Goeckel, "Multi-Differential Slightly Frequency-Shifted Reference Ultra-wideband (UWB) Radio," in *Information Sciences and Systems, 2006 40th Annual Conference on*, 2006, pp. 615–620.

[35] M. Win and R. Scholtz, "Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communications," *Communications, IEEE Transactions on*, vol. 48, no. 4, pp. 679–689, 2000.

[36] D. Goeckel and Q. Zhang, "Slightly frequency-shifted reference ultra-wideband (UWB) radio: TR-UWB without the delay element," in *Military Communications Conference, 2005. MILCOM 2005. IEEE*, 2005, pp. 3029–3035 Vol. 5.

[37] J. Tellado-Mourelo, "Peak to average power reduction for multi-carrier modulation," Ph.D. dissertation, Stanford University, 1999.

[38] D. G. Luenberger, *Optimization by vector space methods*. New York: Wiley, 1990.

[39] H. Boland and H. Mousavi, "Security issues of the IEEE 802.11b wireless LAN," in *Electrical and Computer Engineering, 2004. Canadian Conference on*, vol. 1, May 2004, pp. 333–336 Vol.1.

[40] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978. [Online]. Available: http://doi.acm.org/10.1145/359340.359342

[41] R. Benson, "The venona story," *National Security Agency Central Security Service, Historical Publications (available via WWW)*, 2001.

[42] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *Information Theory, IEEE Transactions on*, vol. 24, no. 4, pp. 451–456, 1978.

[43] G. Caire and D. Tuninetti, "The throughput of hybrid-ARQ protocols for the Gaussian collision channel," *Information Theory, IEEE Transactions on*, vol. 47, no. 5, pp. 1971–1988, 2001.

[44] P. Wu and N. Jindal, "Performance of hybrid-arq in block-fading channels: A fixed outage probability analysis," *Communications, IEEE Transactions on*, vol. 58, no. 4, pp. 1129–1141, April 2010.

[45] X. Tang, R. Liu, P. Spasojevi, and H. Poor, "On the Throughput of Secure Hybrid-ARQ Protocols for Gaussian Block-Fading Channels," *Information Theory, IEEE Transactions on*, vol. 55, no. 4, pp. 1575–1591, April 2009.

[46] X. Tang, R. Liu, and P. Spasojevic, "An Achievable Secrecy Throughput of Hybrid-ARQ Protocols for Block fading Channels," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, 2007, pp. 1311–1315.

[47] Y. Abdallah, M. Latif, M. Youssef, A. Sultan, and H. El-Gamal, "Keys Through ARQ: Theory and Practice," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 737–751, 2011.

[48] J. G. Proakis, *Digital Communications*. McGraw-Hill, 1995.

[49] A. Scaglione, D. Goeckel, and J. Laneman, "Cooperative communications in mobile ad hoc networks," *Signal Processing Magazine, IEEE*, vol. 23, no. 5, pp. 18–29, Sept 2006.

[50] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity. Part I. System description," *Communications, IEEE Transactions on*, vol. 51, no. 11, pp. 1927–1938, Nov 2003.

[51] J. Laneman, D. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *Information Theory, IEEE Transactions on*, vol. 50, no. 12, pp. 3062–3080, Dec 2004.

[52] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *Signal Processing, IEEE Transactions on*, vol. 58, no. 3, pp. 1875–1888, March 2010.

[53] M. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper," in *Information Theory Workshop, 2009. ITW 2009. IEEE*, Oct 2009, pp. 110–114.

[54] E. Tekin and A. Yener, "The General Gaussian Multiple-Access and Two-Way Wiretap Channels: Achievable Rates and Cooperative Jamming," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[55] T. M. Cover and J. Thomas, *Elements of Information Theory*. Wiley, 1991.

[56] X. Liu, "Outage Probability of Secrecy Capacity over Correlated Log-Normal Fading Channels," *Communications Letters, IEEE*, vol. 17, no. 2, pp. 289–292, 2013.

[57] M. Ho, V. Somayazulu, J. Foerster, and S. Roy, "A differential detector for an ultra-wideband communications system," in *Vehicular Technology Conference, 2002. VTC Spring 2002. IEEE 55th*, vol. 4, 2002, pp. 1896–1900 vol.4.

[58] H. Zhang and D. Goeckel, "Generalized transmitted-reference UWB systems," in *Ultra Wideband Systems and Technologies, 2003 IEEE Conference on*, 2003, pp. 147–151.

[59] Q. Zhang and D. Goeckel, "Multiple-Access Slightly Frequency-Shifted Reference Ultra-Wideband Communications for Dense Multipath Channels," in *Communications, 2007. ICC '07. IEEE International Conference on*, 2007, pp. 1083–1088.

[60] H. Joshi, Z. Lai, K. Morrison, C. Capar, and D. Goeckel, "Optimization of frequency-shifted reference ultrawideband systems," in *Signals, Systems and Computers, 2008 42nd Asilomar Conference on*, 2008, pp. 1996–2000.

[61] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[62] M. Dehghan, D. Goeckel, M. Ghaderi, and Z. Ding, "Energy Efficiency of Cooperative Jamming Strategies in Secure Wireless Networks," *Wireless Communications, IEEE Transactions on*, vol. 11, no. 9, pp. 3025–3029, September 2012.

[63] J. Talbot and D. Welsh, *Complexity and Cryptography: An Introduction*. Cambridge University Press, 2005.

[64] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339–348, May 1978.

[65] P. Pinto, J. Barros, and M. Win, "Physical-layer security in stochastic wireless networks," in *Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on*, Nov 2008, pp. 974–979.

[66] Y. Liang, H. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, June 2009, pp. 1189–1193.

[67] P. Gupta and P. Kumar, "The capacity of wireless networks," *Information Theory, IEEE Transactions on*, vol. 46, no. 2, pp. 388–404, Mar 2000.

[68] O. Koyluoglu, C. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," in *Information Theory and Applications Workshop (ITA), 2010*, Jan 2010, pp. 1–4.

[69] M. Haenggi, "The secrecy graph and some of its properties," in *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, July 2008, pp. 539–543.

[70] O. Gungor, J. Tan, C. Koksal, H. El-Gamal, and N. Shroff, "Secrecy Outage Capacity of Fading Channels," *Information Theory, IEEE Transactions on*, vol. 59, no. 9, pp. 5379–5397, Sept 2013.

[71] U. Maurer, "Secret key agreement by public discussion from common information," *Information Theory, IEEE Transactions on*, vol. 39, no. 3, pp. 733–742, May 1993.

[72] Y. Liang, H. Poor, and S. Shamai, "Secure Communication Over Fading Channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[73] A. Juels, "RFID security and privacy: a research survey," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 381–394, Feb 2006.

[74] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc networks," *Communications Magazine, IEEE*, vol. 40, no. 10, pp. 70–75, Oct 2002.

[75] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *Wireless Communications, IEEE*, vol. 11, no. 1, pp. 38–47, Feb 2004.

[76] N. Potlapally, S. Ravi, A. Raghunathan, and N. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *Mobile Computing, IEEE Transactions on*, vol. 5, no. 2, pp. 128–143, Feb 2006.

[77] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, July 2008, pp. 524–528.

[78] R. Wilson, D. Tse, and R. Scholtz, "Channel Identification: Secret Sharing Using Reciprocity in Ultrawideband Channels," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 3, pp. 364–375, Sept 2007.

[79] B. Zhao and M. Valenti, "Practical relay networks: a generalization of hybrid-ARQ," *Selected Areas in Communications, IEEE Journal on*, vol. 23, no. 1, pp. 7–18, Jan 2005.

[80] M. Zorzi, R. Rao, and L. Milstein, "ARQ error control for fading mobile radio channels," *Vehicular Technology, IEEE Transactions on*, vol. 46, no. 2, pp. 445–455, May 1997.

[81] W. Diffie and M. Hellman, "Privacy and authentication: An introduction to cryptography," *Proceedings of the IEEE*, vol. 67, no. 3, pp. 397–427, March 1979.

[82] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete Memoryless Interference and Broadcast Channels With Confidential Messages: Secrecy Rate Regions," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2493–2507, June 2008.

[83] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J. M. Merolla, "Applications of LDPC Codes to the Wiretap Channel," *Information Theory, IEEE Transactions on*, vol. 53, no. 8, pp. 2933–2945, Aug 2007.

[84] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure Broadcasting Over Fading Channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2453–2469, June 2008.

[85] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-Theoretically Secret Key Generation for Fading Wireless Channels," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 2, pp. 240–254, June 2010.

[86] E. Ekrem and S. Ulukus, "Secrecy in Cooperative Relay Broadcast Channels," *Information Theory, IEEE Transactions on*, vol. 57, no. 1, pp. 137–155, Jan 2011.

[87] J. Vilela, M. Bloch, J. Barros, and S. McLaughlin, "Wireless Secrecy Regions With Friendly Jamming," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 2, pp. 256–266, June 2011.

[88] P. Cuff, "A Framework for Partial Secrecy," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, Dec 2010, pp. 1–5.

[89] Z. Ding, K. Leung, D. Goeckel, and D. Towsley, "Opportunistic Relaying for Secrecy Communications: Cooperative Jamming vs. Relay Chatting," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 6, pp. 1725–1729, June 2011.